

# DMRV DUNA MENTI REGIONÁLIS VÍZMŰ ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG



## EU5602

### Adatvédelmi – adatbiztonsági szabályzat ELJÁRÁSI UTASÍTÁS

**ENGEDÉLY NÉLKÜLI MÁSOLÁSA NEM MEGENGEDETT!  
BELSŐ HASZNÁLATRA**

<b>TULAJDONOS NEVE:</b>	<b>A PÉLDÁNY SORSZÁMA:</b>
<input type="text"/>	<input type="text"/>
<b>BEOSZTÁSA:</b>	<b>ÁTVÉTEL IDŐPONTJA:</b>
<input type="text"/>	<input type="text"/>
<b>SZERVEZETI EGYSÉG</b>	<b>ÉRVÉNYESÍTŐ PECSÉT HELYE</b>
<input type="text"/>	<input type="text"/>

A **DMRV Zrt. MSZ EN ISO 9001:2015 és MSZ EN ISO 14001:2015** SZABVÁNYOK SZERINT MŰKÖDŐ INTEGRÁLT MINŐSÉG – ÉS KÖRNYEZETIRÁNYÍTÁSI RENDSZERÉNEK DOKUMENTUMA, A **DMRV Zrt.** TULAJDONA.

JELEN DOKUMENTUMBAN TALÁLHATÓ SZÖVEGRÉSZEK, ÁBRÁK, TÁBLÁZATOK SZELLEMI TERMÉKNEK MINŐSÜLNEK. ÁTVÉTELŰK, MÁSOLÁSUK, ILLETVE BÁRMILYEN MÓDON TÖRTÉNŐ FELHASZNÁLÁSUK CSAK A **DMRV Zrt.** ÍRÁSBELI ENGEDÉLYÉVEL LEHETSÉGES.

EU5602\_v5.docx

	<b>BEOSZTÁS</b>	<b>NÉV</b>	<b>DÁTUM</b>	<b>ALÁÍRÁS</b>
<b>KÉSZÍTETTE</b>	-	L Tender-Consulting Kft.	2018. 05. 15.	s. k.
<b>ELLENŐRIZTE</b>	JOG	dr. Maklári Gábor h.	2018. 05. 17.	Dávidné dr. Lajtos Gyöngyike
<b>ELLENŐRIZTE</b>	SMI	Holczer Szabolcs	2018. 05. 18.	s. k.
<b>ELLENŐRIZTE</b>	KIG	dr. Páris Zoltán	2018. 05. 18.	s. k.
<b>ELLENŐRIZTE</b>	GIG	dr. Kovács Tamás	2018. 05. 22.	s. k.
<b>ELLENŐRIZTE</b>	MIG	Balogh Zsolt	2018. 05. 23.	s. k.
<b>JÓVÁHAGYTA</b>	VIG	Virág László	2018. 05. 24.	s. k.

**JELEN DOKUMENTUM 2018. 05. 25-ÉN LÉP HATÁLYBA.**



## TARTALOMJEGYZÉK

<b>1.</b>	<b>ALKALMAZÁSI TERÜLET .....</b>	<b>5</b>
<b>2.</b>	<b>CÉL.....</b>	<b>5</b>
<b>3.</b>	<b>FOGALMAK, RÖVIDÍTÉSEK.....</b>	<b>5</b>
<b>4.</b>	<b>FELELŐS .....</b>	<b>9</b>
<b>5.</b>	<b>CSATLAKOZÓ DOKUMENTUMOK .....</b>	<b>10</b>
<b>5.1.</b>	<b>KÜLSŐ DOKUMENTUMOK: .....</b>	<b>10</b>
<b>5.2.</b>	<b>BELSŐ DOKUMENTUMOK: .....</b>	<b>11</b>
<b>6.</b>	<b>FOLYAMATLEÍRÁS .....</b>	<b>11</b>
<b>6.1.</b>	<b>AZ ADATKEZELÉS SZABÁLYAI.....</b>	<b>11</b>
6.1.1.	Személyazonosító igazolványok fénymásolása.....	13
<b>7.</b>	<b>A Zrt. adatvédelmi rendszere.....</b>	<b>14</b>
<b>8.</b>	<b>Adatvédelmi incidens kezelése .....</b>	<b>14</b>
<b>8.1.</b>	<b>Adatvédelmi incidens észlelése és jelentése.....</b>	<b>14</b>
<b>8.2.</b>	<b>Adatvédelmi incidens kivizsgálása, értékelése .....</b>	<b>15</b>
<b>8.3.</b>	<b>Az adatvédelmi incidens nyilvántartása .....</b>	<b>15</b>
<b>8.4.</b>	<b>Az adatvédelmi incidens bejelentése a Hatóság részére .....</b>	<b>15</b>
<b>8.5.</b>	<b>Az érintettek tájékoztatása az adatvédelmi incidensről .....</b>	<b>16</b>
<b>9.</b>	<b>Rendszeres tréningek .....</b>	<b>16</b>
<b>10.</b>	<b>Hatásvizsgálat.....</b>	<b>17</b>
<b>11.</b>	<b>Előzetes konzultáció .....</b>	<b>17</b>
<b>12.</b>	<b>Érdekmérlegelés .....</b>	<b>18</b>
<b>13.</b>	<b>Adatbiztonsági szabályok .....</b>	<b>19</b>
<b>13.1.</b>	<b>Fizikai védelem .....</b>	<b>19</b>
<b>13.2.</b>	<b>Informatikai védelem .....</b>	<b>19</b>
<b>14.</b>	<b>Álnevesítés .....</b>	<b>20</b>
<b>15.</b>	<b>Beépített adatvédelem.....</b>	<b>20</b>
<b>16.</b>	<b>Oktatás és tréningrendszer.....</b>	<b>21</b>
<b>17.</b>	<b>Az érintettek jogainak érvényesítése .....</b>	<b>22</b>
<b>18.</b>	<b>Adatkezelések .....</b>	<b>23</b>
<b>18.1.</b>	<b>Felhasználói adatok kezelése .....</b>	<b>24</b>
<b>18.2.</b>	<b>Ügyfélszolgálati adatkezelések .....</b>	<b>27</b>



18.2.1.	Panaszkezelés .....	27
18.2.1.1.	Szóban, személyesen tett bejelentés .....	28
18.2.1.2.	Nem személyesen tett bejelentés .....	28
18.2.1.3.	Telefonos eléréssel működtetett ügyfélszolgálat .....	28
18.2.1.4.	E-mailes panaszok.....	28
18.2.2.	Közös szabályok.....	28
<b>18.3.</b>	<b>Hátralékkezelés .....</b>	<b>29</b>
<b>19.</b>	<b>Pénzügyi adatkezelés.....</b>	<b>30</b>
<b>19.1.</b>	<b>Közüzemi szolgáltatással összefüggő adatkezelés .....</b>	<b>30</b>
<b>19.2.</b>	<b>Irattározás.....</b>	<b>30</b>
<b>20.</b>	<b>Személyügyi adatkezelések .....</b>	<b>30</b>
<b>20.1.</b>	<b>Munkára jelentkezők adataival kapcsolatos adatkezelés .....</b>	<b>30</b>
20.1.1.	A Zrt.-hez történő jelentkezés folyamata .....	30
20.1.2.	A beérkező önéletrajzokkal kapcsolatos közös szabályok .....	31
20.1.3.	A beérkező önéletrajzokra vonatkozó különös szabályok.....	31
20.1.4.	Az ajánlás útján érkező önéletrajzokra vonatkozó különös szabályok.....	31
<b>20.2.</b>	<b>Munkaviszonnyal kapcsolatos adatkezelés .....</b>	<b>32</b>
20.2.1.	Személyazonosító igazolványok fénymásolása.....	32
20.2.2.	Egészségügyi alkalmassággal kapcsolatos egészségügyi adatok kezelése .....	32
20.2.3.	A munkaviszony fenntartásával és megszűnésével kapcsolatos adatkezelések.....	32
20.2.4.	A munkaviszonnyal kapcsolatos adatkezelésekre vonatkozó nyilatkozatok .....	32
20.2.5.	A munkavállalók oktatása .....	33
20.2.6.	Harmadik személy munkaviszonnyal kapcsolatosan megadott adatai.....	33
<b>20.3.</b>	<b>A munkavállalók ellenőrzésével kapcsolatos adatkezelés .....</b>	<b>35</b>
20.3.1.	Céges eszközök ellenőrzése .....	35
20.3.2.	Céges e-mail címek ellenőrzése .....	35
20.3.3.	Internethasználat ellenőrzése .....	35
20.3.4.	Céges autók nyomon követése .....	36
20.3.5.	Munkára alkalmas állapot munkavédelmi vizsgálata .....	36
<b>21.</b>	<b>Vagyonvédelem.....</b>	<b>38</b>
<b>21.1.</b>	<b>Kamerafigyelés.....</b>	<b>38</b>
21.1.1.	Az elektronikus megfigyelőrendszerrel készített felvételek törlésének módja és határideje .....	39
21.1.2.	Az elektronikus megfigyeléssel kapcsolatos garanciális szabályok.....	39
21.1.3.	Az érintettek tájékoztatása .....	39
21.1.4.	A Zrt. munkavállalóinak tájékoztatása .....	39
21.1.5.	A kameraképek megtekintése .....	39
21.1.6.	A kameraképek zárolása.....	40
21.1.7.	Zárolási jogosultsággal rendelkező személyek.....	40
<b>21.2.</b>	<b>Elektronikus beléptetés.....</b>	<b>41</b>
21.2.1.	Vendég beléptetés .....	41
<b>21.3.</b>	<b>Vagyonvédelmi rendkívüli események .....</b>	<b>42</b>
<b>21.4.</b>	<b>Vagyonvédelmi ellenőrzések .....</b>	<b>42</b>
<b>22.</b>	<b>Honlap üzemeltetéssel kapcsolatos adatkezelés .....</b>	<b>42</b>



23.	<b>A KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGA .....</b>	<b>43</b>
24.	<b>Adatvédelmi nyilvántartás .....</b>	<b>43</b>
25.	<b>ELLENŐRZÉS.....</b>	<b>44</b>
	<b>ESEMÉNYTÁBLÁZAT .....</b>	<b>45</b>

## 1. ALKALMAZÁSI TERÜLET

- A szabályzat hatálya kiterjed a DMRV Zrt. minden szervezeti egységénél folytatott valamennyi személyes adatokat tartalmazó adatkezelésre.
- Jelen utasítás hatályba lépésével egyidejűleg az **EU5602 utasítás 4. kiadása hatályát veszti.**
- Jelen utasításban szereplő űrlapok az utasítás közzétételétől kezdődően alkalmazandók.

## 2. CÉL

- E szabályzat célja, hogy az érintettek megfelelő tájékoztatást kaphassanak a Zrt. által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatkezelésbe esetlegesen bevont adatfeldolgozó nevről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.
- E szabályzattal a Zrt. biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést, és azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.
- A szabályzat célja továbbá, hogy a Zrt.-nél biztosítsa az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.) előírásai alapján a közérdekű adatok nyilvánosságát.

## 3. FOGALMAK, RÖVIDÍTÉSEK

- **VIG** - vezérigazgató
- **KIG** - koordinációs igazgató
- **MIG** - műszaki igazgató
- **GIG** - gazdasági igazgató
- **JOG** - Jogi Osztály / - vezető
- **SMI** - Stratégiai és Minőségirányítási Csoport / - vezető
- **Lásd még IMKK 2. és 3. fejezet!**
- **Infotv.** - Információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény
- **GDPR vagy Rendelet** - az Európai Parlament és Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
- **Mt.** - a munka törvénykönyvéről szóló 2012. évi I. törvény
- **Mvt.** - a munkavédelemről szóló 1993. évi XCIII. törvény
- **Ptk.** - a polgári törvénykönyvről szóló 2013. évi V. törvény
- **Sztv.** - a számvitelről szóló 2000. évi C. törvény
- **Szvtv.** - a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény
- **NAIH vagy Hatóság** - Nemzeti Adatvédelmi és Információszabadság Hatóság

**Adatállomány:** az egy nyilvántartásban kezelt adatok összessége.

**Adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik.

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

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

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

**Adatkezelés korlátozása:** a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

**Adatmegsemmisítés:** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.

**Adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

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

**Adatvédelmi incidens:** a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

**Adatzárolás:** az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

**Adatmegjelölés:** az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

**Álnevesítés:** a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják és technikai, szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

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

**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.

**Biometrikus adat:** egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.



**Címzett:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.

**EGT-állam:** az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez.

**Egészségügyi adat:** egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

**Érintett:** azonosított vagy azonosítható természetes személy.

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

**Érintett felügyeleti hatóság:** az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

- az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
- az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
- panaszt nyújtottak be az említett felügyeleti hatósághoz.

**Felügyeleti hatóság:** egy tagállam által a GDPR 51. cikknek megfelelően létrehozott független közhatalmi szerv.

**Genetikai adat:** egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

**Harmadik fél:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.

**Harmadik ország:** minden olyan állam, amely nem EGT-állam;

**Képviselő:** az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra a Rendelet értelmében háruló kötelezettségek vonatkozásában.

**Kötelező erejű vállalati szabályok:** a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ.

**Különleges adat:**

- o a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselési szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
- o az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

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

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

**Nyilvántartási rendszer:** a személyes adatok bármely módon – centralizált, decentralizált, funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

**Nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele.

**Profilalkotás:** személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére, illetve előrejelzésére használják.

**Releváns és megalapozott kifogás:** a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy a Rendeletet megsértették-e, illetve hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a Rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét.

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

**Személyes adat-nyilvántartó rendszer (nyilvántartó rendszer):** személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető.

**Személyes adatok határokon átnyúló adatkezelése:**

- o személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
- o személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket.



**Tevékenységi központ:**

- az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira, eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;
- az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra a Rendelet szerint meghatározott kötelezettségek vonatkoznak.

**Tiltakozás:** az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;

**Vállalkozás:** gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is.

**Vállalkozáscsoport:** az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások.

## 4. FELELŐS

Jelen utasítás folyamatábrát nem tartalmaz. A felelőségeket, és felelősöket, ahol a szükséges, szöveges formában adjuk meg. Az utasítás végrehajtásában az alábbi munkakörök, az alábbi kiemelt felelősséggel vesznek részt:

A **vezérigazgató** adatvédelemmel kapcsolatos feladatai:

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

Az **adatvédelmi tisztviselő** adatvédelemmel kapcsolatos feladatai:

- a) segítséget nyújt az érintett jogainak biztosításában;
- b) minden év január 15-ig jelentést készít a vezető tisztségviselő részére a Zrt. adatvédelmi feladatainak végrehajtásáról;
- c) jogosult jelen szabályzat betartását az egyes szervezeti egységeknél ellenőrizni;
- d) vezeti az adattovábbítási nyilvántartást;
- e) részt vesz a NAIH által szervezett adatvédelmi tisztviselők konferenciáján;
- f) figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását;
- g) közreműködik a NAIH-tól a Zrt.-hez érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;
- h) általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg;

- i) tájékoztatást és szakmai tanácsot ad a Zrt. adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban;
- j) ellenőrzi az adatvédelmi jogszabályoknak, valamint a Zrt. belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosságnövelését és képzését, valamint a kapcsolódó auditokat is;
- k) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
- l) együttműködik a NAIH-val;
- m) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint bármely egyéb kérdésben konzultációt folytat le a Hatósággal;
- n) vezeti az adatvédelmi incidensek kivizsgálását;
- o) jelenti az adatvédelmi incidenseket a Hatóság felé.

Az **informatikus adatvédelemmel** kapcsolatos feladatai:

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

A **szervezeti egységvezető** felelős:

- a) Az adatvédelemért és az adatvédelmi feltételek szervezeti egységén belüli biztosításáért és ellenőrzéséért.

A **valamennyi személyes adatkezeléssel foglalkozó munkatárs** felelős:

- a) Jelen szabályzatban foglaltak alkalmazásáért és betartásáért.

## 5. CSATLAKOZÓ DOKUMENTUMOK

### 5.1. KÜLSŐ DOKUMENTUMOK:

- Vonatkozó további jogszabályok és egyéb kötelező előírások elérhetők a DMRV Zrt. intranet hálózatán.

## 5.2. BELSŐ DOKUMENTUMOK:

- DMRV Zrt. Ügyrendje
- DMRV Zrt. Szervezeti és Működési Szabályzata (SZMSZ)
- **EU4202** Dokumentumok készítésének és kezelésének, valamint elosztásának folyamata
- **EU4203** Ügyiratkezelési szabályzat, irattári terv, cégbélyegzők használata
- **EU4204** Informatikai Biztonsági Szabályzat + Segédletei
- **EU5505** Összeférhetetlenségi szabályzat
- **EU6103** Selejtezési szabályzat
- **EU6113** Alaptevékenységen kívüli Számlázási szabályzat + Segédlet
- **EU6201** A képzés szabályozása
- **EU6401** Vagyonvédelmi szabályzat + Segédlet
- **EU7202** Közüzemi szolgáltatási szerződéskötés folyamata
- **EU8307** Informatikai rendszerek helyreállítási utasítása
- **EU8401** Alkalmazott statisztikák
- **EU8501** Helyesbítő, megelőző tevékenység
- **MU5601** Közérdekű adatkérések rendjét rögzítő szabályzat
- **EU7207** Ügyfélszolgálati Szabályzat + Normagyűjtemény
- **Ü56002** Szabályzat dinamikusan változó adatkezelési rendszerlemeiről
- **Ü56003** Titoktartási nyilatkozat
- **Ü56004** Adatfeldolgozói szerződés
- **Ü56005** Adatvédelmi incidens-nyilvántartó
- **Ü56006** Adatvédelmi incidens értesítési lista
- **Ü56007** Adatvédelmi hatásvizsgálat elkészítéséhez használatos segédanyag
- **Ü56012** Adatvédelmi érdekmérlegelési teszt
- **Ü56013** Adatmegsemmisítési jegyzőkönyv
- **Ü56014** Adatvédelmi tájékoztató ügyfelek részére
- **Ü56015** Panaszfelvételi helyszínen kihelyezendő ügyfél-tájékoztató
- **Ü56016** Adatvédelmi tájékoztató telefonos ügyfélszolgálaton
- **Ü56017** Válaszlevél adatbázisba kerülő önéletrajzra
- **Ü56018** Munkavállalói nyilatkozat ajánláskor
- **Ü56019** Válaszlevél nem az érintettől érkező önéletrajzra
- **Ü56020** Hozzá tartozói nyilatkozat adatkezelésről
- **Ü56021** Adatvédelmi tájékoztató munkavállalók részére
- **Ü56022** Kamerával megfigyelt terület
- **Ü56023** Betekintési joggal rendelkező személyek nyilvántartása
- **Ü56024** Jegyzőkönyv a kamerás képekbe történő betekintéshez
- **Ü56025** Jegyzőkönyv a kamerás képek zárolásról
- **Ü56026** Zárolási joggal rendelkező személyek nyilvántartása
- **Ü56027** Honlapra feltöltendő adatvédelmi tájékoztató
- Lásd **IMKK 9.2. fejezet**, valamennyi integrált rendszer dokumentum megtalálható a DMRV Zrt. intranet hálózatán

## 6. FOLYAMATLEÍRÁS

### 6.1. AZ ADATKEZELÉS SZABÁLYAI

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

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



A Zrt. személyes adatot csak meghatározott célból, jog gyakorlása vagy kötelezettség teljesítése érdekében kezel, a cél eléréséhez szükséges minimális mértékben és ideig. Az adatkezelés minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatok törlésre kerülnek. A törlésről a Zrt.-nek az adatot ténylegesen kezelő munkavállalója gondoskodik. A törlést a munkavállaló felett munkáltatói jogköröket ténylegesen gyakorló személy és az adatvédelmi tisztviselő ellenőrizheti. Az adatvédelmi tisztviselő neve és elérhetősége az **Ü56002** dokumentumban található.

A Zrt. személyes adatot csak az érintett előzetes hozzájárulása, szerződéses kötelezettség teljesítése, törvény, illetve törvényi felhatalmazás, létfontosságú érdek, vagy jogos érdek érvényesítése alapján kezel.

A Zrt. a faji, vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, vagy szakszervezeti tagságra utaló személyes adatokat, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatokat, továbbá egészségügyi adatokat és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatokat (a továbbiakban együtt: a személyes adatok különleges kategóriái) a GDPR tiltása alapján nem kezel.

A személyes adatok különleges kategóriájába eső adatokat a Zrt. az alábbi esetekben kezelheti:

- a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy a 3.5. pontban meghatározott tilalom nem oldható fel az érintett hozzájárulásával;
- b) az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;
- c) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
- d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;
- e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;
- g) az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;
- h) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá a GDPR 9. cikk (3) bekezdésben említett feltételekre és garanciákra figyelemmel;
- i) az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és



az orvostechikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;

j) az adatkezelés a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

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

A Zrt. szervezeti egységeinél adatkezelést végző alkalmazottak és a Zrt. megbízásából az adatkezelésben részt vevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat üzleti titokként megőrizni. A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek Titoktartási nyilatkozatot tenni **(Ü56003)**.

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

A Zrt. megbízásából adatfeldolgozói tevékenységet végző természetes, vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségek az adatfeldolgozóval kötött megbízási szerződésben érvényesítendőek. Az adatfeldolgozóval a Zrt. a GDPR 28. cikk (3) bekezdése által előírt Adatfeldolgozói szerződést köt **(Ü56004)**.

### 6.1.1. Személyazonosító igazolványok fénymásolása

A Zrt. – összhangban a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH vagy Hatóság) álláspontjával – nem készít fénymásolatot személyazonosító igazolványokról. A hatósági okmányról készített fénymásolat nem alkalmas a természetes személyek azonosítására, mivel az egyén személyes jelenléte elengedhetetlen a hatósági igazolvány alapján történő személyazonosításhoz. Az arcképes hatósági igazolvány értelemszerűen csak akkor rendelkezik bizonyító erővel, ha annak alapján a Zrt. megbizonyosodhat arról, hogy az igazolványon szereplő személy képmása és az igazolványt felmutató személy megegyeznek. Egy hatósági igazolványról készített másolat nem rendelkezik bizonyító erővel arról, hogy hiteles másolata egy érvényes hatósági igazolványnak.

Az adatrögzítés és az adatminőség elvének megtartása céljából a Zrt. azonban az azonosító igazolványokról maszkolt fénymásolatot (vagy szkennelt képet – együtt: fénymásolat) készíthet. A fénymásolás során a Zrt. az igazolvány csak azon részeit hagyja fénymásolásra alkalmas, a továbbiakban olvasható állapotban, amely adatokat az érintett egyébként is köteles magáról megadni. A fénymásolat ebben az esetben az adategyeztetés céljából készül. A fénymásolatot a Zrt. azonnal és visszavonhatatlanul törli vagy megsemmisíti, a maszkolt igazolvány-fénymásolatokon szereplő adatok a Zrt. által kijelölt HR munkatársa általi összehasonlítását, de legkésőbb a fénymásolat készültét követő 30 nap elteltével.



## 7. A Zrt. adatvédelmi rendszere

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

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

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

A Zrt. adatvédelmi rendszerének felügyeletét a vezető tisztségviselő látja el egy általa kijelölt adatvédelmi tisztviselő útján.

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

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

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

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

## 8. Adatvédelmi incidens kezelése

### 8.1. Adatvédelmi incidens észlelése és jelentése

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

Amennyiben az adatvédelmi incidens érinti a Zrt. informatikai rendszerét is, akkor a bejelentést az informatikusnak is meg kell küldeni.

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

## 8.2. Adatvédelmi incidens kivizsgálása, értékelése

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

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

Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel az adatvédelmi tisztviselő az informatikussal, valamint egyéb, a vizsgálat lefolytatásához szükséges munkatársak bevonásával lefolytatja a vizsgálatot.

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

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

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

A vizsgálatot legkésőbb a bejelentésnek az adatvédelmi tisztviselőhöz érkezésétől számított 72 órán belül be kell fejezni és a vizsgálat eredményéről a Zrt. vezérigazgatóját az adatvédelmi tisztviselő tájékoztatja.

## 8.3. Az adatvédelmi incidens nyilvántartása

Az adatvédelmi incidensről az adatvédelmi tisztviselő nyilvántartást vezet.

A nyilvántartás tartalmazza:

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

Az adatvédelmi incidensnyilvántartás **(Ü56005)** pontos vezetéséről, aktualizálásáról az adatvédelmi tisztviselő gondoskodik.

## 8.4. Az adatvédelmi incidens bejelentése a Hatóság részére

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



A hatósági bejelentésnek tartalmaznia kell:

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

## 8.5. Az érintettek tájékoztatása az adatvédelmi incidensről

Ha a vizsgálat eredményeként megállapítást nyer, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket és erről a Zrt. vezérigazgatóját is értesíti. Az értesítendőök listáját az **Ü56006. sorszámú** dokumentum tartalmazza.

Nem kell az érintetteket tájékoztatni:

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

## 9. Rendszeres tréningek

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



## 10. Hatásvizsgálat

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

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

A Zrt. jelen szabályzat **Ü56007. sorszámú** dokumentumban leírt szempontrendszer figyelembevételével elvégzi a hatásvizsgálatot.

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

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

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

Szükséges a kockázatforrások feltárása, melyen belül meg kell határozni a kockázati preventív és korrektív célkezelés elemeit, az erőforrás-kezelés rendszerét, továbbá el kell különíteni az objektív és szubjektív kockázati elemeket.

Az elemzés során el kell jutni a teljes kockázatértékelési rendszer kialakításáig, amelyben teljes kockázatpotenciál és kockázat prioritási sorrend (nem az intézkedési rendszerrel azonos) megállapításának kell megtörténnie. Az elemzés menetét és eredményeit írásba kell foglalni.

A kockázatpotenciálnál meg kell határozni a valószínűség szempontjából

- kicsi
  - közepes
  - és nagy bekövetkezésű kockázatokat,
- illetve horderő szempontjából
- kicsi
  - közepes
  - és nagy horderejű kockázatokat.

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

## 11. Előzetes konzultáció

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



A konzultáció kezdeményezése során a Zrt. csatolja:

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

## 12. Érdekmérlegelés

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

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

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

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

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

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

A teszt eredményéről az érintettek tájékoztatást kapnak, melyből egyértelműen kiderül, hogy mely jogos érdek alapján és miért tekinthető arányos korlátozásnak az, hogy a Zrt. az érintett beleegyezése nélkül kezeli a személyes adatot, tehát a Zrt. adatkezeléséhez fűződő jogos érdeke miatt múlja felül az érintett érdekeit, illetve jogait. A Zrt. tájékoztatja az érintetteket a hozzájárulás hiányára tekintettel alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről.

Nem írható elő az ellentétes érdekek és jogok közötti súlyozás eredménye anélkül, hogy eltérő eredményt tenne lehetővé a Zrt. az adott eset sajátos körülményeire tekintettel, ezért a Zrt. minden egyes esetben külön érdekmérlegelési tesztet végez el.

Lehetséges forgatókönyv, melytől való eltérés jogát a Zrt. fenntartja:

1. lépés: a Zrt. a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.
2. lépés: a Zrt. a jogos érdekét a lehető legpontosabban meghatározza.



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

A Zrt. jelen szabályzat **Ü56012 sorszámú** dokumentumában leírt szempontrendszer figyelembevételével végzi el az érdekmérlegelést.

## 13. Adatbiztonsági szabályok

### 13.1. Fizikai védelem

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

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

Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, úgy a Zrt. intézkedik a papír megsemmisítéséről. Ebben az esetben a Zrt. kijelöl egy munkavállalót, aki a megsemmisítésért felelős. A megsemmisítésért felelős munkavállaló a megsemmisítéssel érintett szervezeti egység bevonásával állítja össze a megsemmisítendő iratcsomagot. A megsemmisítésen háromtagú megsemmisítési bizottság köteles részt venni. A megsemmisítésről adatmegsemmisítési jegyzőkönyvet kell kitölteni (**Ü56013**). A bizottság tagjai ellenőrzik, hogy megsemmisítésre valóban azok az iratok kerülnek, amelyeket az adatmegsemmisítési jegyzőkönyvben feltüntettek.

Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére a papírok megsemmisítési szabályai irányadóak.

### 13.2. Informatikai védelem

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Zrt. a hatályos informatikai biztonsági szabályzatában foglaltak szerint jár el.



## 14. Álnevesítés

Az álnevesítés a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, mivel a Társaság az ilyen további információt külön tárolja, technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

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

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

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

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

## 15. Beépített adatvédelem

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

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

A Társaság a tudomány és technológia állása, a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei, céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével, mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket –

- a) a személyes adatok álnevesítését és titkosítását;
- b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;



c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást - hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

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

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

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

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

## 16. Oktatás és tréningrendszer

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

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

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

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

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



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

## 17. Az érintettek jogainak érvényesítése

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

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

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

Az Adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

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

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

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

A személyes adatot törölni kell, ha

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



- f) a személyes adatok gyűjtésére a 16 éven aluli gyermekek részére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor;
- g) ha az adatkezelő nyilvánosságra hozta a személyes adatot, és a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték úgy azt törölni köteles, valamint az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Az érintett tiltakozhat személyes adatának kezelése ellen:

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

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

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

Az Adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt, illetve az általa vagy az általa igénybe vett adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is megtéríti. Az adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Ugyanígy nem téríti meg a kárt, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

Ha az Adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be NAIH-nál (1125 Budapest, Szilágyi Erzsébet fasor 22/C.) és élhet - lakóhelye vagy tartózkodási helye szerint illetékes törvényszéknél - bírósági jogorvoslati jogával.

## 18. Adatkezelések

Az adatkezelés helye:

- Vác Kodály Z. út 3. (központ)
- Vác Derecske u. 4/a.
- Szentendre, Kalászi út 2.
- Gödöllő, Sík S. u. 7.
- Balassagyarmat, Rákóczi út 134.



## 18.1. Felhasználói adatok kezelése

### Általános szabályok

A szolgáltatási tevékenységével kapcsolatosan a Zrt. betartja a víziközmű szolgáltatásról szóló 2011. évi CCIX. törvény (a továbbiakban: Vksztv.) előírásait. A törvény az alábbiak szerint jogalapot biztosít a szolgáltatási tevékenységhez kapcsolódó adatkezelések végzésére.

A Zrt., mint víziközmű-szolgáltató, az alábbi célokból kezelhet adatokat:

- a törvényben meghatározott tevékenységének végzése,
- a tevékenységének végzéséhez szükséges műszaki berendezések létesítésére, üzemeltetésére vonatkozó szerződés megkötése, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése,
- szerződésben meghatározott díjak számlázása,
- szerződésből eredő követelések érvényesítése,
- együttműködési és adatszolgáltatási kötelezettségek teljesítése,
- az ingatlan víziközmű-rendszerbe történő bekötetése,
- a védendő fogyasztókkal kapcsolatos adatok kezelése, nyilvántartása, az őket megillető kedvezmények biztosítása érdekében.

A Zrt. a fenti célokból a felhasználó azonosításához szükséges és elégséges, a törvény szerint a szerződés tartalmát képező személyes adatot, továbbá az ingatlan azonosításához szükséges helyrajzi számot és címet kezeli.

A felhasználó azonosításához az alábbi adatokat kezelheti a Zrt. természetes személy felhasználó esetén:

- név,
- lakcím,
- anyja neve,
- születési hely és idő.

A védendő fogyasztók esetében a kezelt adatok köre a fenti személyes adatokon túl:

a szociálisan rászoruló, vagy a fogyatékkal élő státuszra, esetleg mindkettő együttes fennállására történő utalás, a különleges bánásmód esetén annak formája, valamint a felhasználó által igénybe vehető kedvezményekre vonatkozó információk.

A védendő fogyasztók adatkezelésére a jogalapot a Vksztv. 61/A. § (1) és (2) bekezdése adja meg.

A védendő fogyasztók köre kétféle lehet:

- szociálisan rászoruló,
- vagy fogyatékkal élő.

A védendő fogyasztók nyilvántartásába való felvételt az érintettnek kell kezdeményeznie a Zrt. nyomtatványán. A kérelemben megadott adatok bekerülnek az ügyfélnyilvántartásba, azonban a jogosultságot alátámasztó egyéb adatokat papíralapon tárolják, és csak az illetékes ügyintéző kezeli.

A rászorultságot alátámasztó információk kezelésére szintén jogszabály ad jogalapot, a vízi közmű-szolgáltatásról szóló törvény felhatalmazása alapján az 58/2013. (II. 27.) számú Kormányrendelet 88/C. és 88/D. §.-ai. Ezen adatok tárolási határideje: a jogosultság megszűnését követő 5 év.

A Zrt. a kezelt személyes adatot haladéktalanul törli, ha

- az adatkezelési cél megszűnt, például a víziközmű-szolgáltatás keretében létrejött jogviszony megszűnik,
- a jogviszonyhoz kapcsolódó követelés érvényesítése megtörtént,
- a jogviszonyhoz kapcsolódó követelés érvényesíthetősége megszűnt.



A törvény rendelkezik az adatok harmadik fél részére történő továbbításáról is, az adat ugyanis átadható:

- annak a természetes személynek vagy gazdálkodó szervezetnek, aki vagy amely az adatkezelő megbízása alapján
  - a szerződés megkötését,
  - a leolvasást,
  - a számlázást,
  - a kézbesítést,
  - a díjfizetések kezelését,
  - a követelések kezelését,
  - a forgalmazás kezelését,
  - a felhasználási helyek műszaki kivitelezését, felülvizsgálatát, ellenőrzését, kikapcsolását,
  - az ügyfélszolgálati tevékenységet végzi;
- a számlázási és forgalmazási jogviták rendezésére jogszabály alapján jogosult szervezeteknek,
- az üzemeltetési szerződés megszűnését követően az ellátásért felelősnek,
- az üzemeltetési szerződés megkötését követően a víziközmű-szolgáltatóknak,
- a közérdekű üzemeltetőnek,
- Magyar Energetikai és Közmű-szabályozási Hivatalnak,
- a fogyasztóvédelmi hatóságnak,
- a járási hivatalnak,
- a bírósági végrehajtásról szóló törvény előírásai szerint a bírósági végrehajtónak,
- a nemzetbiztonság, a honvédelem és a közbiztonság védelme, a közvadás bűncselekmények üldözése céljából az arra hatáskörrel rendelkező nemzetbiztonsági szerveknek, nyomozó hatóságnak, ügyésznek, valamint bíróságnak.

### Ügyfelek adatainak kezelése

A Zrt. a közműszolgáltatás ellátása céljából ügyféladatbázist üzemeltet, amelyben az ügyfelekre vonatkozóan bekerül minden információ: szerződési, számlázási adatok, és a panaszbejelentésekkel kapcsolatos információk, amely adatokhoz az illetékesek férnek hozzá jelszóval.

Az ügyfél minden megadott adatát a Zrt. rögzíti adatbázisában. Abban az esetben, ha az ügyfél több adatot ad meg, mint ami az adott ügy elintézéséhez feltétlenül szükséges, akkor a Zrt. az adatminimalizálás céljából a felesleges adatokat törli.

A tulajdonosváltást több csatornán is bejelentheti a régi és az új ügyfél: mind személyesen, mind írásban.

Személyesen az ügyfélszolgálaton teheti meg a bejelentést az ügyfél. Csatolható emellett a tulajdonosváltást bizonyító okirat is, így adásvételi szerződés, bérleti szerződés, tulajdoni lap, birtokbaadási jegyzőkönyv, kezességvállalás, halotti anyakönyvi kivonat, jegyzőkönyv hagyatéki eljárásról, árverezési jegyzőkönyv. Emellett meghatalmazás és szolgáltatási szerződés is mellékelhető.

Amennyiben a Zrt. Üzletszabályzata alapján az ügyintézéshez az ügyintézésre okot adó tényt bizonyító okiratot is kér, úgy az okiratról készült másolatot az ügyintézésre rendszerezett nyomtatványhoz csatolva egészen addig tárolja, ameddig az ügyintézésrel érintett eljárásból eredő polgári jogi igények fennállhatnak. Az adatok átvezetéséhez nem szükséges adatokat (*pl. adásvétel alapján megtörtént ügyfélváltás esetén a vételárat*) a Zrt. törli.

### Leolvasás, felhasználási helyek műszaki kivitelezése

A Zrt. fenntartja a jogot, hogy a Vksztv. 61. § (3) a)-ban kapott törvényi felhatalmazás szerint a leolvasással és a felhasználási helyek műszaki kivitelezésével (így különösen a mellékvízmérők cseréjét) harmadik felet bízson meg, a harmadik félnek az érintettek személyes adatait átadja.



Erre jogalapot a Vksztv. 61. § (3) a) teremt, miszerint az *adatkezelés céljához szükséges adatok átadhatóak az adatkezelő megbízása alapján a leolvasást, a felhasználási helyek műszaki kivitelezését végző természetes személynek és gazdálkodó szervezetnek.*

A Zrt. az adatátadással egyidejűleg értesíti az érintettet.

A mérőállásokat telefonon keresztül (automata rögzíti), személyesen ügyfélszolgálati irodában, honlapon keresztül, valamint ügyfélszolgálati központi e-mail címre tudják bejelenteni.

Aktuális fogyasztásról szolgáltatott információ érkezhethet:

- fogyasztó diktálása alapján,
- társasházak esetén közös képviselő által leadott adatok alapján,
- tényleolvasás alapján.

A társasházak esetében vagy a közös képviselő gyűjti össze a lakók fogyasztási adatait és egységesen ő diktálja be a fogyasztási adatokat a Zrt. felé, vagy a felhasználók maguk diktálják az adatot. A lakók egymás fogyasztási adatait nem ismerhetik meg.

A Zrt. alkalmazottai által történő leolvasás során, ha a fogyasztót nem találják otthon, az első alkalommal értesítőt hagynak, amely értesítő tartalmazza, hogy a leolvasást végző munkatárs mikor járt ott, és mikor jön legközelebb. Az értesítőt minden esetben az ügyfél postaládájába dobják be.

A Zrt. honlapján is tehető mérőállás bejelentés és egyéb ügyintézés.

Az ügyintézés során megadandó adatok:

- ügyfél neve,
- azonosító száma,
- fogyasztási hely címe
- a vízmérő gyári száma, és a vízmérő állása,
- locsolómérő adatai,
- ügyfél e-mail címe,
- telefonszáma.

A felhasználói adatok kezelése, (víziközmű szolgáltatásból eredő ügyféladat kezelés, ivóvíz szolgáltatás, szennyvízelvezetés és tisztítás vízóra leolvasás, mérőóra csere kapcsán történő adatkezelések).

**adatkezelés célja:** a közműves ivóvízellátás és szennyvízelvezetés, ügyféladatbázis üzemeltetése a polgári jogi jogok és kötelezettségek teljesítése céljából

**kezelt adatok köre:** közüzemi szolgáltatás kapcsán felhasználói azonosító, ügyfél neve, anyja neve, születési helye és ideje, e-mail címe, telefonszáma, szolgáltatás helye (ingatlan helyrajzi száma, ivóvíz fogyasztási és szennyvízelvezetés helye), bejelentések, panaszok adatai, fizetési adatok (így különösen bankszámlaszám), mellékvízmérő adatai, adatváltozást bizonyító okiratok.

A védendő fogyasztókra vonatkozó adatok: a szociálisan rászoruló, vagy a fogyatékkal élő státuszra, esetleg mindkettő együttes fennállására történő utalás, a különleges bánásmód esetén annak formája, valamint a felhasználó által igénybe vehető kedvezményekre vonatkozó információk.

**adatkezelés jogalapja:** törvényi kötelezettség [a víziközmű-szolgáltatásról szóló 2011. évi CCIX. törvény 61. § és 61/A. §] és az érintett hozzájárulása [GDPR 6. cikk (1) a) pontja], valamint az 58/2013. (II. 27.) Kormányrendelet 88/C. § és 88/D. §-a



**adattárolás határideje:** polgári jogi igények elévüléséig

**adattárolás módja:** elektronikusan és papíralapon (a védendő fogyasztók esetében a jogosultságot alátámasztó iratok papíralapon kerülnek tárolásra)

A számlázás cégen belül történik, és a számlák kinyomtatása is a Zrt.-nél zajlik.

**Ezen adatkezelésekhez kapcsolódó nyilvántartási számok:** NAIH-56593/2012, NAIH-56592/2012, NAIH56591/2012

A műszaki karbantartásra, mérőóra cserére, hibabejelentésre, számlázásra vonatkozóan történik szerződésen alapuló adatátadás **az adatok további felhasználása céljából** Önkormányzatok és Társszolgáltatók részére, mérőóra leolvasásra vonatkozóan történik adatátadás **adatfeldolgozás céljából** megbízott vállalkozóknak.

## 18.2. Ügyfélszolgálati adatkezelések

A panaszok megtételére több mód is rendelkezésére áll az ügyfeleknek, így szóbeli, írásbeli és telefonos panasztételre is van lehetőség. Az ügyfélszolgálat a fogyasztóvédelemről szóló 1997. évi CLV. törvény előírásai szerint üzemel.

### 18.2.1. Panaszkezelés

A Zrt. a panaszkezelést a mindenkori Üzletszabályzatban meghatározottak szerint végzi. A panasz megtételére lehetőséget biztosító helyszínen a Zrt. tájékoztatót helyez el.

Panaszok esetén az adatkezelés a fogyasztóvédelemről szóló 1997. évi CLV törvény (a továbbiakban: Fgytv.) 17/A-C. §-ában meghatározottak szerint történik.

Lehetőség van arra, hogy az ügyfél helyett meghatalmazottja jelenjen meg az ügyfélszolgálaton ügyet intézni. Ebben az esetben csak a Polgári Törvénykönyvről szóló 2013. évi V. törvény szerinti írásos meghatalmazás bemutatása szükséges, így a meghatalmazott adatai is kezelésre kerülnek a Zrt. részéről.

Amennyiben az érintett a panasz kezelésével nem ért egyet, vagy annak azonnali kivizsgálása nem lehetséges, akkor a panaszról jegyzőkönyvet készítenek, melyet az ügyfélnyilvántartásból nyomtatnak ki. A jegyzőkönyv egy másolati példányát a Zrt.-nek át kell adnia a fogyasztónak.

A panaszról felvett jegyzőkönyv a következőket kell, hogy tartalmazza:

- az ügyfél neve;
- az ügyfél lakcíme, székhelye, illetve amennyiben szükséges, levelezési címe;
- a panasz előterjesztésének helye, ideje, módja;
- az ügyfél panaszának részletes leírása, a panasszal érintett kifogások elkülönítetten történő rögzítésével, annak érdekében, hogy az ügyfél panaszában foglalt valamennyi kifogás teljes körűen kivizsgálásra kerüljön;
- a panasszal érintett szerződés száma, ügytől függően ügyfélszám;
- az ügyfél által bemutatott iratok, dokumentumok és egyéb bizonyítékok jegyzéke;
- a jegyzőkönyvet felvevő személy és az ügyfél aláírása (utóbbi formai elem személyesen közölt szóbeli panasz esetén elvárt);
- a jegyzőkönyv felvételének helye, ideje.



### 18.2.1.1. Szóban, személyesen tett bejelentés

Az ügyintéző, az ügyfélnyilvántartásból nyomtatott ügyfélszolgálati jegyzőkönyvön veszi fel – lehetőség szerint gépi úton – az adatokat. A dokumentumon a bejelentés módja, kelte és tárgya, a bejelentő adatai (név, cím,), a fogyasztó adatai (név, fogyasztási hely, fogyasztó azonosító), a panasz leírása szerepel.

A dokumentumot mind az ügyintéző, mind a bejelentő ellátja aláírásával, amelynek másolati példányát a bejelentő is megkapja.

### 18.2.1.2. Nem személyesen tett bejelentés

Nem személyes bejelentés tehető telefonon vagy írásban, postai úton.

### 18.2.1.3. Telefonos eléréssel működtetett ügyfélszolgálat

A Zrt. az Fgytv. 17/B. § (3) szerinti telefonos eléréssel működtetett ügyfélszolgálatot üzemeltet. A Zrt. az ügyfélszolgálathoz beérkező valamennyi telefonon tett szóbeli panaszt, valamint az ügyfélszolgálat és a fogyasztó közötti telefonos kommunikációt hangfelvétellel rögzít. Minden hangfelvételt egyedi azonosítószámmal lát el, amelyet öt évig őriz meg.

A hangfelvételt a fogyasztó kérésére díjmentesen bocsátja a fogyasztó rendelkezésre.  
A felvételek külső szerveren kerülnek tárolásra.

A Zrt. a hangfelvétel készítésével, megőrzésével és rendelkezésre bocsátásával kapcsolatos kötelezettségéről, továbbá az egyedi azonosítószámról a fogyasztót a telefonos ügyintézés kezdetekor tájékoztatja.

A vállalkozás a panaszról felvett jegyzőkönyvet és a válasz másolati példányát öt évig köteles megőrizni, és azt az ellenőrző hatóságoknak kérésükre bemutatni.

### 18.2.1.4. E-mailes panaszok

Online úton panasztételre van lehetőség a [www.dmrvzrt.hu](http://www.dmrvzrt.hu) oldalon az alábbiak szerint:

Panaszokat a honlapon és az Üzletszabályzatban is feltüntetett központi e-mail címre ([dmrvzrt@dmrvzrt.hu](mailto:dmrvzrt@dmrvzrt.hu)) lehet küldeni.

## 18.2.2. Közös szabályok

Az ügyfélszolgálat minden esetben írásba foglalja a vállalkozás panasszal kapcsolatos álláspontját és intézkedéseit indokolással ellátva, a fogyasztónak a panasz beérkezését követő tizenöt napon belül megküldi, kivéve, ha a fogyasztó panaszát szóban közli és a vállalkozás az abban foglaltaknak nyomban eleget tesz.

**adatkezelés célja:** panaszok rögzítése, vizsgálása, elbírálása

**kezelt adatok köre:** az ügyfél neve; lakcíme, levelezési címe, a panasz előterjesztésének helye, ideje, módja, az ügyfél panaszának részletes leírása, a telefonon felvett adatok esetében az egyedi azonosító szám, az ügyfél által bemutatott iratok, dokumentumok és egyéb bizonyítékok és azok jegyzéke, a jegyzőkönyvet felvevő személy és a személyesen közölt szóbeli panasz esetén az ügyfél aláírása, a jegyzőkönyv felvételének helye, ideje, az ügyféllel való kapcsolattartási e-mail cím, telefonszám.



**adatkezelés jogalapja:** a GDPR (1) a) szerinti érintetti hozzájárulás a fogyasztóvédelmi törvény 17/A-C. §-ban meghatározott jogalappal

**adattárolás határideje:** a vállalkozás a panaszról felvett jegyzőkönyvet, a válasz másolati példányát és az egyedi azonosítószámmal ellátott hangfelvételt öt évig megőrzi [Fgytv. 17/A. § (7) és 17/B. § (3)]

### 18.3. Hátralékkezelés

A hátralékról az első információt a számlán szereplő aktuális egyenleg értékéből kapja a felhasználó, részletezés nélkül. Következő lépésként a hátralékos felhasználók a számlázási rendszerből előállított, számlánkénti részletezésű fizetési felszólítást kapnak a jogkövetkezmények ismertetésével, amelyek ajánlott postai küldeményként kerülnek kiküldésre. Ennek eredménytelensége (kiegyenlítés, illetve részletfizetési engedély kérelem elmaradása) esetén ismételten a hátralékos részletező tértivevényes fizetési felszólítást küld a Zrt.

További eredménytelenség esetén újabb, tértivevényes levélben – a hátralék részletezésével – kap tájékoztatást az adós felhasználó az ivóvíz szolgáltatás korlátozásának (lakosság) vagy szüneteltetésének (közület) tervezett kezdési időpontjáról. Amennyiben a hátralék rendezése eddig az időpontig sem történik meg, a Zrt. kísérletet tesz a korlátozás/szüneteltetés végrehajtására.

A szankcionálás megszüntetésére a teljes tartozás kiegyenlítését követő 24 órán belül intézkedés történik. Kiegyenlítésnek a pénzüsszeg beérkezési időpontja számít.

Az eredménytelen felszólításokat követően a korlátozási/szüneteltetési intézkedés helyett vagy azzal párhuzamosan a várható eredményesség mérlegelése alapján behajtási eljárást kezdeményez a Zrt. amely fizetési meghagyási szakaszból és szükség esetén végrehajtási szakaszból áll.

A hátralékosok adatai továbbításra kerülnek követeléskezelő társaságok., közjegyzők és bírósági végrehajtók felé.

**adatkezelés célja:** adatkezelő szolgáltatási területén az adatok kezelése hátralékkezelés céljából.

**kezelt adatok köre:** név; leánykori név, anyja neve; születési hely; születési idő; állandó lakhely; telefonszám; levelezési cím, fogyasztási hely

**adatkezelés jogalapja:** Vksztv. 61. § (3) a) szerinti törvényi felhatalmazás

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

**adattárolás módja:** elektronikusan

Az ügyfelek adatkezelésére és a panaszkezeléssel összefüggő adatkezelésekre vonatkozóan adatvédelmi tájékoztató készült, melynek célja az ügyfelek előzetes tájékoztatása az adatkezelésekről. (Ü56014. Adatvédelmi tájékoztató ügyfelek részére, Ü56015. Panaszfelvételi helyszínen kihelyezendő ügyfél tájékoztató). Ez az adatvédelmi tájékoztató a Zrt. honlapján közzétételre és valamennyi ügyfélszolgálaton jól látható helyen kifüggesztésre kerül.

A Zrt. által használt nyomtatványokon, - amelyeken az ügyfelek személyes adatai feltüntetésre kerülnek, az alábbi adatvédelmi tájékoztató szöveget kell elhelyezni:



**A DMRV Zrt. felhívja ügyfelei figyelmét, hogy a nyomtatvány kitöltése során felvételre kerülő személyes adatokat az adatvédelmi szabályzatában (EU5602) és az ügyfeleknek szóló tájékoztatóban (Ü56014) foglaltaknak megfelelően kezeli, melyeket megtekinthet a cég honlapján ([www.dmrvzrt.hu](http://www.dmrvzrt.hu))**

Személyes ügyintézés esetén a nyomtatványokat és ezzel együtt a rajta szereplő adatvédelmi tájékoztatót alá kell írni az ügyféllel és azt az ügyintézői ívben el kell helyezni.

Telefonos ügyfélszolgálat esetében egy telefonos gépi hang egy rövid tájékoztatást ad, mellyel az ügyfél tájékoztatása megtörténik arról, hogy adatai milyen feltételek mellett kerülnek rögzítésre. A Zrt. honlapján részletes tájékoztatót kell közzétenni (Ü56016 Adatvédelmi tájékoztató telefonos ügyfélszolgálaton).

## 19. Pénzügyi adatkezelés

### 19.1. Közüzemi szolgáltatással összefüggő adatkezelés

A Zrt. fenntartja a jogot, hogy a Vksztv. 61. § (3) a)-ban kapott törvényi felhatalmazás értelmében - miszerint az *adatkezelés céljához szükséges adatok átadhatóak az adatkezelő megbízása alapján a számlázást a kézbesítést végző természetes személynek és gazdálkodó szervezetnek* - a közüzemi szolgáltatással összefüggő tevékenysége során a számlázásba és a kézbesítésbe harmadik felet vonjon be, a harmadik félnek az érintettek személyes adatait átadja.

A Zrt. az adatátadással egyidejűleg értesíti az érintettet.

### 19.2. Irattározás

A Zrt. fenntartja a jogot, hogy a pénzügyi adatkezelése során kiállított számlák kezelésével (így különösen azok kategorizálásával, tárolásával, selejtezésével) harmadik felet bízjon meg. A harmadik fél a számlák kezelése során köteles betartani a Zrt. iratkezelési szabályait.

**adatkezelés célja:** számlázás

**kezelt adatok köre:** magánszemély esetén név, cím, fogyasztási hely, számlázással kapcsolatos adatok, fogyasztási adatok, egyéni vállalkozó beszállító esetén neve, címe, adószáma, számlavezető pénzügyintézet neve, bankszámlaszáma

**adatkezelés jogalapja:** a 2000. C. tv. 169. § (1)-(2)-ben szereplő törvényi rendelkezés

**adattárolás határideje:** 8 év [Sztv. 169. § (1)-(2)]

## 20. Személyügyi adatkezelések

### 20.1. Munkára jelentkezők adataival kapcsolatos adatkezelés

#### 20.1.1. A Zrt.-hez történő jelentkezés folyamata

A megfelelő munkavállaló kiválasztásáért a szakmai vezető a felelős, így a jelen adatkezeléssel összefüggő feladatok ellátása során a Zrt. belső adatvédelmi felelősével együttműködve köteles az érintettek jogait biztosítani.



### 20.1.2. A beérkező önéletrajzokkal kapcsolatos közös szabályok

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

Főszabály szerint az önéletrajzokat későbbi felhasználás céljából - a később megüresedő vagy betöltendővé váló pozíciók miatt - kategorizálja a Zrt. és egy adatbázist épít belőlük. Az adatbázisba kerülő adatokat egy év elteltével meg semmisíti lévén ennyi idő elteltével már vélhetően nem relevánsak a munkakeresés szempontjából az adatok.

### 20.1.3. A beérkező önéletrajzokra vonatkozó különös szabályok

A Társaság minden esetben (a meghírdetett álláshelyekre, vagy csak a későbbi álláslehetőség reményében) válaszlevelet küld a jelentkezőnek, amelyben tájékoztatja az adatkezelés tényéről, jogalapjáról és az adatkezelés elleni tiltakozás formáiról. A „Válaszlevél adatbázisba kerülő önéletrajzra” című válasz a szabályzat **Ü56017.** sz. mellékletét képezi.

### 20.1.4. Az ajánlás útján érkező önéletrajzokra vonatkozó különös szabályok

A Zrt. ismeri és elismeri a munkavállalói ajánlás rendszerét. A Zrt. bármely munkavállalója ajánlhatja ismerősét általánosságban vagy egy konkrét pozícióra – ekkor azonban a Zrt. minden esetben nyilatkoztatja munkavállalóját (**Ü56018.**) arról, hogy felhatalmazással rendelkezik az adatok érintettjétől, hogy azokat feltárja a Zrt. előtt. Jelen nyilatkozatot az adott CV tárolási határidejéig megőrzi, majd ezt követően a CV-n szereplő adatokkal együtt megsemmisíti.

Amiatt azonban, mert az érintett hozzájárulását – a munkavállalói nyilatkozattal együtt is – a Zrt. csak vélelmezni tudja, ezért minden ilyen esetben tájékoztató levelet küld az ajánlott személy számára, amelyben tájékoztatja az adatkezelés tényéről, jogalapjáról és az adatkezelés elleni tiltakozás formáiról. A „Válaszlevél nem az érintettől érkező önéletrajzra” című válasz a szabályzat **Ü56019.** sz. melléklete.

***A CV alapján kiválasztott érintett adatainak további kezelése (úgy mint: alkalmasság eldöntése) már a munkaviszony létesítése céljából történik, így az azzal kapcsolatos adatkezelést a 20.2. pont taglalja.***

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

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

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

**adattárolás határideje:** az adatbázisba kerüléstől számított egy év

**adattárolás módja:** papíralapon és elektronikusan

## 20.2. Munkaviszonnal kapcsolatos adatkezelés

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

### 20.2.1. Személyazonosító igazolványok fénymásolása

Az adatrögzítés és az adatminőség elvének megtartása céljából a Zrt. az újonnan belépő vagy adatot módosító munkavállalói azonosító igazolványairól maszkolt fénymásolatot (vagy szkennelt képet – együtt: fénymásolat) készít. A fénymásolás során a Zrt. az igazolvány csak azon részeit hagyja fénymásolásra alkalmas, a továbbiakban olvasható állapotban, amely adatokat a munkavállaló a belépése során egyébként is köteles magáról megadni. A fénymásolat ebben az esetben a NÜSZ Zrt. felé továbbítás céljából készül. A szkennelt kép a SAP HCM modulban rögzítésre kerül, majd a fénymásolat megsemmisítésre, a szkennelt kép törlésre kerül legkésőbb a fénymásolat készültét követő 30 nap elteltével.

### 20.2.2. Egészségügyi alkalmassággal kapcsolatos egészségügyi adatok kezelése

Az egészségügyi alkalmassággal kapcsolatos adatokat a Zrt. nem ismeri meg, és nem kezeli egyetlen érintett adatát a célon túlterjeszkedő mértékben. A Zrt. az egészségügyi alkalmasság eldöntése céljából egészségügyi szolgáltatótól származó alkalmassági eredmény alapján dönt az adott (leendő) munkavállaló egészségügyi alkalmasságáról. A Zrt. csak az egészségügyi alkalmasság tényét bizonyító adatot kezeli.

### 20.2.3. A munkaviszony fenntartásával és megszűnésével kapcsolatos adatkezelések

A Zrt. munkavállalóiról személyi, illetve bér- és munkaügyi nyilvántartást vezet.

A személyi nyilvántartás a munkaviszonyra vonatkozó tények dokumentálására szolgáló adatkezelés. A személyzeti nyilvántartás adatai a munkavállaló munkaviszonyával kapcsolatos tények megállapítására és statisztikai adatszolgáltatásra használhatók fel. A személyi nyilvántartás Zrt. valamennyi munkavállalójának adatait tartalmazza.

A munkavállalók adatkezelésének jogalapja a törvényi felhatalmazás (munka törvénykönyvről szóló 2012. évi I. törvény), illetve az érintett hozzájárulása [GDPR 6. cikk (1) a)] ad jogalapot.

### 20.2.4. A munkaviszonnal kapcsolatos adatkezelésekre vonatkozó nyilatkozatok

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





## 20.2.5. A munkavállalók oktatása

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

## 20.2.6. Harmadik személy munkaviszonnal kapcsolatosan megadott adatai

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

Abban az esetben, ha a munkavállaló harmadik személy adatait adja meg, úgy nyilatkozni köteles **(Ü56020.)**, hogy a harmadik személy adatainak megadására vonatkozóan felhatalmazással rendelkezik.

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

### **kezelt adatok köre:**

munkavállaló kapcsán

- azonosító száma,
- neve,
- születési neve,
- születési helye és ideje,
- állampolgársága,
- anyja születési neve,
- lakóhelyének címe,
- tartózkodási helye (amennyiben eltérő a lakóhelytől),
- magán-nyugdíjpénztári
  - o tagság ténye,
  - o belépés ideje (év, hó, nap)
  - o bank neve és kódja
- adóazonosító jele,
- társadalombiztosítási azonosító jele (TAJ szám),
- nyugdíjas törzsszám (nyugdíjas munkavállaló esetén),
- folyószámla száma,
- munkaviszony kezdő napja,
- biztosítási jogviszony típusa,
- heti munkaórák száma,
- telefonszáma,



- családi állapota,
- végzettséget igazoló okmány másolati példánya,
- munka-alkalmassági egészségügyi igazolás,
- munkaköre,
- orvosi alkalmasság ténye,
- a leszámolást követően a munkaköri alkalmassági záró orvosi vizsgálat elvégzésének ténye,
- meghatározott munkakörben vezetési engedély kategóriánkénti egészségügyi alkalmasságának lejártának időpontja,
- a csökkent munkaképességű munkavállaló csökkent munkaképességét megalapozó szakértői határozat,
- főálláson kívüli munkavégzés esetén
  - o jogviszony jellege,
  - o munkáltató neve és székhelye,
  - o a főálláson kívüli munkahelyen teljesített havi átlagos munkaidő,
  - o elvégzendő tevékenység,
- az Mt. 120. § alapján járó pótszabadság igénybevételével kapcsolatosan
  - o a rehabilitációs szakértői szerv legalább ötven százalékos mértékű egészségkárosodását megállapítását igazoló okmány fénymásolata
  - o fogyatékosági támogatásra jogosultságot igazoló okmány fénymásolata,
  - o vakok személyi járadékára jogosultságot igazoló okmány fénymásolata,

pótszabadság, családi adókedvezmény igénybe vétele, adómentes természetbeni juttatásnak minősülő kedvezményes utazási igazolvány igénylésének vagy adómentes iskolakezdési támogatás céljából munkavállaló 16. életévét be nem töltött hozzátartozójának

- születési helye és ideje,
- lakcíme,
- anyja neve
- társadalombiztosítási azonosító jele (TAJ szám)
- adóazonosító jele,
- 

megváltozott munkaképességű munkavállalók esetében a fenti adatkör kiegészül az alábbiakkal:

- az Infotv. 3. § 3. pontja alapján különleges személyes adatnak minősülő egészségügyi állapotra vonatkozó adatokat tartalmazó dokumentumok:
  - o szakértői bizottság szakvéleménye /ORSZI - Országos Rehabilitációs és Szociális Szakértői Intézet/
  - o határozat a megváltozott munkaképességről

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

**adattárolás határideje:** az adatkezelés céljának megvalósulásáig, főszabály szerint

- munkaviszonnyal kapcsolatos jogosultságokkal és kötelezettségekkel kapcsolatosan a munkaviszony megszűnéséig,
- munkaviszonyból fakadó jogosultságokkal kapcsolatosan a nyugdíjfolyósításról szóló jogszabályokban meghatározott határideig



**adatkezelés módja:** papíralapon és elektronikusan

A munkavállalók részére adatkezelési tájékoztató készült, melynek célja a munkavállalók előzetes tájékoztatása az adatkezelésekről (**Ü56021.** Adatvédelmi tájékoztató munkavállalók részére).

### **20.3. A munkavállalók ellenőrzésével kapcsolatos adatkezelés**

A munkáltató a munkaviszonnyal összefüggő magatartása körében ellenőrizheti a munkavállalókat a munkaviszonnyal összefüggésben. Az ellenőrzésre a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban Mt.) 11. § (1)-(2) bekezdése ad jogalapot.

A Zrt. az Mt.-ben meghatározott jogalappal ellenőrzi munkavállalóit: a Zrt. – összhangban információbiztonsági szabályaival – előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak.

#### **20.3.1. Céges eszközök ellenőrzése**

A Zrt. a munkavállalóknak indokolt esetben, munkavégzés céljára biztosít számítógépet, e-mail címet és internet-hozzáférést. A használat szabályairól és az ellenőrzés lehetőségéről a munkavállalókat a Zrt. előzetesen írásban tájékoztatja – a tájékoztatás alapját az informatikai rendszer használatáról szóló mindenkori szabályzat adja.

Mivel a Zrt. tulajdonát képező személyi számítógépeket és laptopokat, céges e-mail címeket a Zrt. munkavégzés céljából biztosítja, így amennyiben a munkavállaló ezen eszközökön magáncélú személyes adatait (pl.: családi fotók, telefonkönyvek, saját adatbázisok stb.) tárolja, úgy a Zrt. a számítógép ellenőrzése során ezeket az adatokat is megismerheti. Ezen adatkezelés ellen kifogással nem élhet a munkavállaló, mert a nem munkavégzés céljából történő, de a Zrt. eszközein való személyes adatok tárolása az adatkezeléshez történő hozzájárulásnak minősül.

Erről (illetve az archiválás és a rendszergazdai tevékenység tényéről) a munkavállalókat az eszközök használata előtt írásban tájékoztatja a Zrt.

#### **20.3.2. Céges e-mail címek ellenőrzése**

A Zrt. munkavállalói mindazon e-mail címeket, amelyekben a Zrt. neve kiterjesztésként benne foglaltatik (...@dmrvzrt.hu), a Zrt. tulajdonát képezik és az ezen címeken folytatott levelezés munkacélú levelezésnek minősül. A fogadott és küldött e-mailek tartalma a Zrt. tulajdonát képezik!

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

Amennyiben a munkavállaló a „...@dmrvzrt.hu” céges e-mail címen található leveleiben magáncélú személyes adatait tárolja, úgy a Zrt. az e-mail cím ellenőrzése során ezeket az adatokat is megismerheti. Ezen adatkezelés ellen kifogással nem élhet a munkavállaló, mert a nem munkavégzés céljából történő, de a céges e-mail címen való személyes adatok tárolása az adatkezeléshez történő hozzájárulásnak minősül.

#### **20.3.3. Internethasználat ellenőrzése**

A fenti szabályok érvényesek az internethasználatra is: az internet használata munkaidőben csak céges célokra engedélyezett. Emiatt az internetezési adatok céges adatoknak minősülnek.



#### 20.3.4. Céges autók nyomon követése

A Zrt. fenntartja a jogot, hogy a tulajdonában lévő autókba nyomkövető rendszert telepít. A gépjármű csak a Zrt. céljaival összefüggésben használható, aminek során a nyomkövető rendszer folyamatosan jelzést ad a gépjármű aktuális pozíciójáról. Mivel a gépjármű használója minden esetben összeköthető a gépjármű aktuális pozíciójával, így ez személyes adattá válik – erről a Zrt. minden esetben tájékoztatja a gépjárművet használó munkavállalót.

**adatkezelés célja:** a Zrt. jogos üzleti érdekeinek megfelelően a munkavállalók Mt. 11. § (1) szerinti ellenőrzése, így különösen a munkavállalónak biztosított számítógép, e-mail cím és internet-hozzáférés ellenőrzése, a céges autók útvonalának ellenőrzése

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

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

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

A személyügyi adatkezelések körében a nem közvetlenül a munkaviszonyból eredeztetett adatkezelések során minden esetben be kell szerezni, a kezeléshez felhasznált nyomtatványba be kell emelni szövegszerűen – az érintett kifejezett hozzájárulását, az adatkezelés céljának és várható időtartamának megjelölésével.

#### 20.3.5. Munkára alkalmas állapot munkavédelmi vizsgálata

Az Mt. 52. § (1) a) kimondja, hogy a munkavállaló a munkáltató által előírt helyen és időben munkára képes állapotban megjelenni.

A munkavédelemről szóló 1993. évi XCIII törvény (a továbbiakban: Mvt.) 2. § (3)-ban kapott felhatalmazás alapján az alábbiak szerint határozza meg az alkoholos befolyásoltságra vonatkozóan az egészséget nem veszélyeztető és biztonságos munkavégzés követelményeinek megvalósítását:

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

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

Jelen szabály alól indokolt esetben csak a vezérigazgató adhat írásos felmentést.



A biztonságos munkavégzés feltételeit veszélyeztetheti a munkára képes állapot hiánya, így az alkoholos befolyásoltság. Emiatt az érintettnek nem csak a munkavégzésre történő megjelenéskor kell munkára képes állapotban lennie, hanem ezt az állapotát egészen a munkaideje lejártáig köteles megőrizni.

A munkavállaló munkája ellátása során nem veszélyeztetheti sem a maga, sem pedig más egészségét és testi épségét.

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

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

A munkavédelmi szabályok betartásának ellenőrzésére a Zrt. munkavédelmi felelőse jogosult, akit a Zrt. vezérigazgatója az Mvt. 57. § (1) szerint jelöl ki. Jelen pont szerinti ellenőrzési jogkörét a munkavédelmi felelős akadályoztatása esetén a kijelölt vagyonvédelmi szolgálat Szvtv. szerinti vagyónőreire delegálhatja. A portaszolgálaton történő ellenőrzést kizárólag a vagyonvédelmi szolgálat munkatársai végzik.

Az alkoholos befolyásoltság ellenőrzése azonban a fentiekkel összhangban sem járhat a munkavállaló emberi méltóságának megsértésével – így a munkavédelmi felelős nem élhet vissza ellenőrzési jogával, illetve azt nem gyakorolhatja annak rendeltetésével ellentétesen, például ha a vizsgálatot naponta többször indok nélkül vagy személyes bosszúból folytatja, de az is jogszerűtlen, ha jogkörrel nem rendelkező személy rendeli el a vizsgálatot.

Az ellenőrzésre jogosult személyek:

- vezérigazgató,
- munkavédelmi felelős,
- a szervezeti egység vezető (osztályvezető, üzemvezető) és helyettesei
- koordinátor, telepvezető,
- szállításvezető

A felsoroltak bármikor elrendelhetik az ellenőrzést, akár az Mvt. 54. § (7) b)-ben kapott felhatalmazás alapján szűrőpróbaszerűen is. Az ellenőrzést a munkavédelmi felelős saját maga végezheti,

Az ellenőrzés pontos menete:

- az ellenőrzésre jogosult bármikor elrendelheti bármely munkavállalóra vonatkozóan az alkoholos ellenőrzést, akár szűrőpróbaszerűen is,
- gyanú esetén az érintett közvetlen munkahelyi vezetője köteles eljárást kezdeményezni,
- az ellenőrzésre jogosult a Zrt. bármely munkavállalójának jogosult elrendelni az ellenőrzést, amennyiben a munkahelyi vezető megjelöli az ellenőrzés indokát és az ellenőrizendő személyt, az ellenőrzésre jogosult azonban jogosult az ellenőrzést megtagadni, amennyiben az intézkedésre okot adó körülményekből egyértelműen arra lehet következtetni, hogy az ellenőrzés nem indokolt,
- a vizsgálatot a munkavállaló személyiségi jogainak megsértése nélkül, két tanú jelenlétében, szondával vagy műszeres szondával kell elvégezni,
- az ellenőrzés tényéről az ellenőrzést végző személy jegyzőkönyvet állít ki, a jegyzőkönyv tartalmi kellékei az ellenőrzés ténye, az ellenőrzésre okot adó körülmény (általános munkavédelmi célú ellenőrzés vagy alkoholos befolyásoltság gyanúja), az ellenőrzéssel érintett személy, az ellenőrzés



- időpontja, az ellenőrzés eredménye, az ellenőrzött személy az ellenőrzés eredményével kapcsolatos jognyilatkozata (elfogadja, nem fogadja el)
- amennyiben a munkavállaló az eredményt nem fogadja el, úgy az üzemorvosnál vagy egyéb egészségügyi szolgáltatónál kezdeményezheti a véralkohol szintjének vérévétellel történő ellenőrzést,
  - amennyiben az ellenőrzés alá fogott munkavállaló nem hajlandó az ellenőrzésre jogosulttal együttműködni és nem veti magát alá az ellenőrzésnek, a az ellenőrzésre jogosult azonnal értesíti a munkavállaló felett munkáltatói jogkörrel rendelkező személyt,
  - az ellenőrzés megtagadása automatikusan munkára alkalmatlan állapotnak minősül az Mvt. 60. § (1) szerint, lévén megtagadja a törvényben foglalt együttműködési kötelezettséget.
  - A szállításvezető csak a gépkocsivezetők, munkagép kezelők ellenőrzésére jogosult az ellenőrzött munkaideje alatt. Gépjárművel történt baleset esetén a gépkocsivezetőt, vagy munkagépkezelőt a helyszínen, vagy a kivizsgáláskor rövid időn belül a telephelyen jogosult ellenőrizni.

Abban az esetben, ha a munkavállaló munkára alkalmatlannak minősül (pozitív eredmény vagy együttműködési kötelezettség megszegése), úgy az ellenőrzést végző személy azonnal köteles értesíteni a munkavállaló felett munkáltatói jogkörrel vagy döntési jogkörrel rendelkező személyt, aki köteles a munkavállalót felmenteni a munkavégzés alól.

**adatkezelés célja:** munkára alkalmas állapot ellenőrzése munkavédelmi célból

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

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

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

**adattárolás módja:** papíralapon és elektronikusan

Az ellenőrzési folyamatról a munkavállalók részére részletes tájékoztató készült, melyet a munkavállalók megismertek.

## 21. Vagyonvédelem

Az őrzés egyrészt vagyonvédelmi biztonsági őrkkel, másrészt távfelügyeleti rendszerben (riasztó távfelügyelet), harmadrészt az **E6401** Vagyonvédelmi Szabályzat és Segédletében előírtak alapján történik. (Személyi védelem, műszaki védelem, elektronikai védelem szerint)

### 21.1. Kamerafigyelés

A személyi és vagyonvédelmi, valamint a megánnymozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: Szvtv.) 31. § -ában meghatározott jogalappal és előírások figyelembe vételével a Zrt. elektronikus megfigyelő rendszert üzemeltet a székhelyén és egyes telephelyein:

- Vác Kodály Z. út 3. (központ)
- Vác Derecske u. 4/a.
- Szentendre, Kalászi út 2.
- Gödöllő, Sík S. u. 7.
- Balassagyarmat, Rákóczi út 134.
- Balassagyarmat, Szennyvíztelep



### **21.1.1. Az elektronikus megfigyelőrendszerrel készített felvételek törlésének módja és határideje**

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

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

### **21.1.2. Az elektronikus megfigyeléssel kapcsolatos garanciális szabályok**

A Zrt. az elektronikus megfigyelőrendszerrel csak a kellő mértékben avatkozik bele az érintettek magánszférájába.

A Zrt. semmilyen indokból és módon nem folytat elektronikus megfigyelést:

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

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

### **21.1.3. Az érintettek tájékoztatása**

Az adatkezelésre vonatkozóan tájékoztató készült, melynek célja az érintettek előzetes tájékoztatása az adatkezelésről (**Ü56022** Kamerával megfigyelt terület). A tájékoztató a megfigyelt területekre történő összes belépési ponton kihelyezésre kerül.

### **21.1.4. A Zrt. munkavállalóinak tájékoztatása**

Az adatkezelésre vonatkozóan munkavállalói tájékoztató készült, melynek célja a előzetes tájékoztatása az adatkezelésről.

### **21.1.5. A kameraképek megtekintése**

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



A Zrt. szervezetrendszerén belül csak a jelen szabályzatban kijelölt személy jogosult a felvételeket megtekinteni.

A Zrt. által megvalósított elektronikus megfigyelés során csak az **Ü56023.** sz. dokumentumban felsorolt személyek rendelkeznek betekintési joggal.

A kamerás képekbe történő betekintésről jegyzőkönyvet kell készíteni (**Ü56024.**).

### **21.1.6. A kameraképek zárolása**

Kamerakép zárolását csak a Zrt. kamerarendszer által megvalósított adatkezelés felügyeletére kijelölt személye — rendelheti el.

Kamerakép zárolását kezdeményezheti

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

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

A zárolásról a lehető legrövidebb időn belül a Zrt. kamerarendszer által megvalósított adatkezelés felügyeletére kijelölt személy - a belső adatvédelmi felelőssel egyetértésben - dönt.

A Zrt. minden, a kamerával rögzített képekből történő zárolásról jegyzőkönyvet vesz fel (**Ü56025.**), amiben rögzíteni kell a betekintés és a zárolás időpontját, célját és a zárolásra okot adó eseményt és a további felhasználás megjelölését.

### **21.1.7. Zárolási jogosultsággal rendelkező személyek**

A Zrt. a zárolásra jogosultak köréről is nyilvántartást vezet (**Ü56026**). A nyilvántartás része a zárolási joggal rendelkező személy neve és beosztása, a zárolási jog kiadásának dátuma, a zárolási jog visszavonásának dátuma. Az adatokat a visszavonástól számított 5 éven keresztül őrzi meg a Zrt..

**adatkezelés célja:** az emberi élet, testi épség, személyi szabadság védelme, vagyonvédelem

**kezelt adatok köre:** az érintett képmása, az elektronikus megfigyelőrendszer által rögzített képekből megszereshető egyéb adatok (így különösen: tartózkodási hely, ehhez kapcsolódó dátum)

**adatkezelés jogalapja:** érintetti hozzájárulás az Szvtv. 30. § (2)-ben foglalt felhatalmazás szerint

**adattárolás határideje:**

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





## 21.2. Elektronikus beléptetés

A Társaság elektronikus beléptető rendszert alkalmaz a székhelyén és egyes telephelyein.

A beléptetés RFID kártyák alkalmazásával történik, mellyel azon a helyen ahol elektronikus beléptető rendszer került alkalmazásra, minden munkavállaló rendelkezik.

A beléptető rendszer a Társaság saját üzemeltetésében van, a belépési adatokra a biztonságtechnikai munkatársak látnak rá, illetve azok a munkavállalók, akik menedzser master hozzáféréssel rendelkeznek. A beléptető rendszer rögzíti és tárolja minden belépési pontra történő belépés és kilépés idejét, valamint az RFID azonosító számát.

A beléptető rendszer vagyonvédelmi célokat szolgál, illetve a belépési jogosultságok ellenőrzéséhez szükséges személyazonosítást szolgálja.

Külső szereplő nem lát rá a belépési adatokra.

A csomagok, zsebek, illetve gépjárművek átvizsgálása, ellenőrzése történhet meg az egyes telephelyekre történő be-vagy kihajtásokkor.

**adatkezelés célja:** ki- és beléptetés során megvalósított vagyonvédelmi ellenőrzés a Zrt. munkavállalói esetében

**kezelt adatok köre:** a be- és a kilépés ideje, a belépő azonosító száma

**adatkezelés jogalapja:** a 2005. évi CXXXIII. törvény 32. §.

**adattárolás határideje:**

- rendszeres belépésnél a belépésre való jogosultság megszűnésekor azonnal, de legkésőbb az adat keletkezésétől számított tizenkét hónap elteltével, alkalmi belépési jogosultság esetén az adat keletkezésétől számított 24 órán belül

**adattárolás módja:** elektronikusan, papír alapon

A beléptetési folyamatról a munkavállalók részére részletes tájékoztató készült, melyet a munkavállalók megismertek.

### 21.2.1. Vendég beléptetés

Vendégek beléptetése szintén RFID kártya kiadásával történik. A kártya átadása előtt papír alapon kerül rögzítésre a kártya tulajdonos neve és az, hogy honnan és kihez érkezett. Rögzítésre kerül a kártyaátadás és a kártyaleadás időpontja is.

**adatkezelés célja:** a be- és kiléptetés során megvalósított vagyonvédelmi ellenőrzés

**kezelt adatok köre:** az érkező személy neve, a fogadó személy neve, belépés, kilépés ideje, a vendég belépő kártya azonosító száma

**adatkezelés jogalapja:** a 2005. évi CXXXIII. törvény 32. §.

**adattárolás határideje:**

- alkalmi belépési jogosultság esetén az adat keletkezésétől számított 24 órán belül

**adattárolás módja:** elektronikusan

### 21.3. Vagyonvédelmi rendkívüli események

Rendkívüli esemény minden olyan, az átlagostól jelentősen eltérő esemény, körülmény, amely az épületben tartózkodó személyek életét, testi épségét vagy az ott található anyagi javakat tekintve súlyos következményekre vezethet vagy reális esélye van annak, hogy vezetni fog és ezzel az objektum működésében komoly zavart okoz.

A területen a megbízott szolgáltató vagyonőrei vesznek fel vagyonvédelmileg releváns eseményekről jegyzőkönyvet. A jegyzőkönyvben az alábbi adatok megadása szükséges: a jegyzőkönyv kitöltésének dátuma, biztonsági szolgálat munkatársának neve, aláírása, vizsgált személy neve, aláírása, vizsgált személy születési neve, születési helye, ideje, anyja neve, lakcíme, tartózkodási helye és a cselekmény leírása. Jelen adatok relatív személyes adatok, azaz az Infotv. szerinti személyes adattá is válhatnak.

**adatkezelés célja:** vagyonvédelmi rendkívüli események kivizsgálása

**kezelt adatok köre:** a jegyzőkönyv kitöltésének dátuma, biztonsági szolgálat munkatársának neve, aláírása, vizsgált személy neve, aláírása, vizsgált személy születési neve, születési helye, ideje, anyja neve, lakcíme, tartózkodási helye és a cselekmény leírása

**adatkezelés jogalapja:** a 2005. évi CXXXIII. törvény 26. §.- a

**adattárolás határideje:** az esemény kivizsgálása, az abból fakadó jogokkal és kötelezettségekkel kapcsolatos igényérvényesítésre nyitva álló határidő

**adattárolás módja:** papíralapon

### 21.4. Vagyonvédelmi ellenőrzések

A Zrt. vagyontárgyainak védelme érdekében az Szvtv. 26. §-ban kapott felhatalmazás alapján csomag-, szekrény- és jármű- és szállítmány-ellenőrzést is végez.

Az ellenőrzést a vagyonőr a szerződésből fakadó kötelezettségei érvényesítése céljából, a tervezett intézkedése okának és céljának közlése mellett akkor végezheti el, ha

- megalapozottan feltehető, hogy az érintett bűncselekményből vagy szabálysértésből származó olyan dolgot tart magánál, amelynek őrzése a vagyonőrnek szerződésből fakadó kötelezettsége,
- e dolgot a felszólítás ellenére sem adja át és
- az intézkedés a jogsértő cselekmény megelőzése, megszakítása érdekében szükséges.

Amennyiben az ellenőrzés pozitív eredménnyel zárul, úgy az ellenőrzésről rendkívüli eseményről szóló jegyzőkönyvet vesz fel a vagyonőr, amelyre vonatkozóan az azzal kapcsolatos adatkezelés szabályai irányadóak (szabályzat 15.3. pontja).

## 22. Honlap üzemeltetéssel kapcsolatos adatkezelés

A Zrt. az alábbi címen <http://www.dmrvzrt.hu/> üzemeltet honlapot, mely honlaphoz bárki kiléte felfedése nélkül hozzáférhet, a honlapon szabadon és korlátozás nélkül szerezhethet információkat. A látogatókról személyhez kötött információkat automatikusan nem gyűjt a weblap, viszont a honlapon több olyan lehetősége is van a látogatóknak, ahol személyes adatokat adhatnak meg. Pl. mérőállás bejelentés, hibabejelentés, vevőszolgálat.

A honlapon elérhető személyes adatok megadását igénylő menüpontokhoz adatkezelési tájékoztató készült **Ü56027**.



**adatkezelés célja:** kapcsolatfelvétel, kapcsolattartás

**adatkezelés jogalapja:** az érintett hozzájárulása

**kezelt adatok köre:** partnerkód név, e-mail cím, fogyasztási hely kódja

**adatok törlésének határideje:** az adatközléstől számított 2 év

**adattárolás módja:** elektronikusan

## 23. A KÖZÉRDEKŰ ADATOK NYILVÁNOSSÁGA

A Zrt. helyi önkormányzati feladatot és jogszabályban meghatározott közfeladatot ellátó szerv, így a feladatkörébe tartozó ügyekben, a közpénzek felhasználására és erre kötött szerződésekre, a piaci szereplők, a magánszervezetek és - személyek részére különleges vagy kizárólagos jogok biztosítására vonatkozóan - köteles elősegíteni és biztosítani a közvélemény pontos és gyors tájékoztatását.

A vezető tisztségviselők, felügyelő bizottsági tagok javadalmazását külön szabályzat rögzíti.

Ha a törvény másként nem rendelkezik, a belső használatra készült, valamint a döntés-előkészítéssel összefüggő adat a kezelését követő húsz éven belül nem nyilvános. Kérelemre az adatok megismerését a szerv vezetője e határidőn belül is engedélyezheti.

A közérdekű adatok nyilvánosságát korlátozhatja továbbá az Európai Unió jogszabálya az Európai Unió jelentős pénzügyi, vagy gazdaságpolitikai érdekére tekintettel, beleértve a monetáris, a költségvetési, az adópolitikai érdeket is.

A Zrt. feladatkörébe tartozó ügyekben köteles biztosítani a közvélemény pontos és gyors tájékoztatását. Az adatokat elektronikusan: internetes honlapon, digitális formában bárki számára díjmentesen kell hozzáférhetővé tenni. A közérdekű adat megismerésére irányuló kérelemnek a Zrt. a kérelem tudomására jutását követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül, közérthető formában tesz eleget. Nem kell közzétenni a közfeladatot ellátó szerv hatáskörébe tartozó döntés meghozatalára irányuló, a döntés megalapozását szolgáló adatokat keletkezéstől számított 10 évig.

Ha a közérdekű adatra vonatkozó kérést a Zrt. nem teljesíti, a kérelmező a bírósághoz fordulhat. A bíróság soron kívül jár el, és ha a kérelemnek helyt ad, határozatában a Zrt-t a kért közérdekű adat közzétételére kötelezi.

A közérdekű adatok nyilvánosságát és az adatkérés rendjét a Zrt.-nél külön szabályzat, a **MU5601** közérdekű adatkérések rendjét rögzítő szabályzat biztosítja.

## 24. Adatvédelmi nyilvántartás

A Zrt.-vel munkaviszonyban álló személyek adatainak a Zrt.-nél történő kezelése olyan személyes adatkezelés, amelyet a törvény alapján nem kell bejelenteni és adatvédelmi nyilvántartásba venni, ugyanakkor az ügyfélkapcsolati jogviszony alapján kezelt adatok bejelentés kötelesek.

A nyilvántartás célja, hogy a polgárok megismerjék, milyen adatkezelő, milyen adatkezeléseket végez.

A nyilvántartást a NAIH vezeti.

Az Adatvédelmi nyilvántartás hatósági nyilvántartásnak minősül. Addig nem kezdhető meg az adatkezelés, míg azt a Hatóság nyilvántartásba nem veszi.



Minden eltérő célú adatkezelést önállóan be kell jelenteni.

A Zrt. köteles bejelenteni nyilvántartásba vétel végett a Hatóságnak:

- adatkezelés célját
- jogalapját
- érintettek körét
- érintettekre vonatkozó adatok leírását
- adatok forrását
- adatok kezelésének időtartamát
- továbbított adatokat, azok célját, jogalapját, fajtáját, címzettjét
- adatkezelő feldolgozó megnevezését, azok helyét, tevékenységét
- alkalmazott technológia jellegét
- adatvédelmi felelős elérhetőségét

A nyilvántartásba vételkor nyilvántartási számot kap a bejelentés. Ezen nyilvántartási számot az adatok minden továbbításánál, nyilvánosságra hozásánál és az érintettnek való kiadáskor fel kell tüntetni.

## 25. ELLENŐRZÉS

Az adatvédelemmel kapcsolatos előírások, így különösen ezen szabályzat rendelkezéseinek betartását a Zrt.-nél adatkezelést végző szervezeti egységek vezetői folyamatosan kötelesek ellenőrizni.

A Zrt.-nél a kezelt adatok ellenőrzését a vezérigazgató és az általa megbízott adatvédelmi felelős és a belső ellenőr bevonásával évente egyszer ellenőrzi.

**ESEMÉNYTÁBLÁZAT**

kiadás száma	kiadás időpontja	változtatott oldal	változtatás leírása
1.	2004. 04. 26.	Összes	Új kiadás
2.	2009. 07. 20.	Összes	Teljes átdolgozás, melynek hatályba lépésével egyidejűleg az EU5602 utasítás 1. kiadása hatályát veszti.
3.	2013. 02. 15.	Összes	Teljes átdolgozás.
4.	2013. 09. 27.	Összes	Ügyfél terekben történt kamera elhelyezés. Munkavállalói adatkezelés kiegészítése.
5.	2018. 05. 15.	Összes	Teljes átdolgozás.