

**MORGEN-RED Kft.**

**Adatkezelési**

**szabályzata**

***GDPR***

**Az Európai Parlament és a Tanács (EU)**

**2016/679 rendelete szerint**

Változat: 1.0

Jóváhagyta:

Dátum: 2018.05.25.

Dokumentum azonosító: [Adatkezelési szabályzat v1.0](file://E:\MIR\Documents%20and%20Settings\TSzanto\Local%20Settings\Temporary%20Internet%20Files\Content.Outlook\Documents%20and%20Settings\TSzanto\Local%20Settings\Temporary%20Internet%20Files\Content.Outlook\Documents%20and%20Settings\TSzanto\Local%20Settings\Temporary%20Internet%20Files\Content.Outlook\Documents%20and%20Settings\TSzanto\Local%20Settings\Documents%20and%20Settings\TSzanto\Local%20Settings\Temporary%20Internet%20Files\Content.Outlook\Documents%20and%20Settings\TSzanto\Local%20Settings\Temporary%20Internet%20Files\Content.Outlook\Loginform%20ISO%209001%202001\Documents%20and%20Settings\szs\Local%20Settings\Documents%20and%20Settings\szs\Application%20Data\Microsoft\Documents%20and%20Settings\Documents%20and%20Settings\Documents%20and%20Settings\Documents%20and%20Settings\szs\Local%20Settings\Temporary%20Internet%20Files\!!!\Minőségirányítási%20kézikönyv%20v3.doc)

Felügyelt egyetlen nyomtatott törzspéldány!

A számítógépes hálózaton minden munkatárs számára megismerhető !

Tartalomjegyzék

[Tartalomjegyzék 2](#_Toc515536301)

[Az Adatkezelési szabályzat változataiban végrehajtott módosítások 5](#_Toc515536302)

[Vezetői nyilatkozat 6](#_Toc515536303)

[1. Bevezetés 7](#_Toc515536304)

[1.1 Az adatkezelési szabályzat célja 7](#_Toc515536305)

[1.2 Hatály 8](#_Toc515536306)

[2. Áttekintés az Európai Parlament és a Tanács (EU) 2016/679 rendeletéről 9](#_Toc515536307)

[2.1 Alapelvek 10](#_Toc515536308)

[2.2 Bizonyítható hozzájárulás 11](#_Toc515536309)

[2.3 Érthető, részletes tájékoztatás, gyors intézkedés 11](#_Toc515536310)

[2.4 Az érintett jogai 12](#_Toc515536311)

[2.5 Az adatkezelő feladatai 13](#_Toc515536312)

[2.6 Az adattovábbítás általános elve 14](#_Toc515536313)

[3. Fogalomtár 15](#_Toc515536314)

[4. Kapcsolódó külső és belső szabályok 23](#_Toc515536315)

[5. Felelősségi körök 25](#_Toc515536316)

[5.1 Szervezeti felépítés 25](#_Toc515536317)

[5.2 Képzés 27](#_Toc515536318)

[6. Felülvizsgálat, ellenőrzés, szakmai kapcsolattartás 28](#_Toc515536319)

[6.1 Felülvizsgálat, ellenőrzés 28](#_Toc515536320)

[6.2 Szakmai kapcsolattartás 28](#_Toc515536321)

[7. Személyes adatok kezelése, nyilvántartás 29](#_Toc515536322)

[7.1 Adatkezelés 29](#_Toc515536323)

[7.1.1 A személyes adatok kezelésére vonatkozó elvek 29](#_Toc515536324)

[7.1.2 Az adatkezelés jogszerűsége 30](#_Toc515536325)

[7.1.3 Munkavállalók adatkezelése 30](#_Toc515536326)

[7.1.3.1 Adatkezelés az érintett hozzájárulása alapján 31](#_Toc515536327)

[7.1.3.2 Adatkezelés jogi kötelezettség teljesítése érdekében 31](#_Toc515536328)

[7.1.3.2.1 Adatkezelés munkaviszony létesítése, teljesítése és kapcsolódó nyilvántartási kötelezettségeknek való megfelelés érdekében 32](#_Toc515536329)

[7.1.3.2.2 Alkalmassági vizsgálatokhoz kapcsolódó adatkezelés 33](#_Toc515536330)

[7.1.3.3 Szerződéshez kapcsolódó adatkezelések 34](#_Toc515536331)

[7.1.3.4 Adatkezelés munkáltatói jogos érdek alapján 34](#_Toc515536332)

[7.1.3.4.1 Álláspályázatok adatkezelése 35](#_Toc515536333)

[7.1.3.4.2 Munkáltatói e-mail cím/fiók használata 36](#_Toc515536334)

[7.1.3.4.3 Munkahelyi internet és wifi használat 37](#_Toc515536335)

[7.1.3.4.4 Munkahelyi számítógép használata 38](#_Toc515536336)

[7.1.3.4.5 Munkáltató által biztosított mobiltelefon, telefon használata 39](#_Toc515536337)

[7.1.4 Jogi kötelezettség teljesítése érdekében történő adatkezelés 40](#_Toc515536338)

[7.1.4.1 Adatkezelés adó- és társadalombiztosítási kötelezettségek teljesítése céljából 40](#_Toc515536339)

[7.1.4.2 Adatkezelés pénzmosás elleni kötelezettségek teljesítése céljából 41](#_Toc515536340)

[7.1.4.3 A Levéltári törvény szerint maradandó értékű iratokra vonatkozó adatkezelés 41](#_Toc515536341)

[7.1.4.4 Fogyasztóvédelmi ügyintézés, reklamációk adatkezelése 42](#_Toc515536342)

[7.1.5 Szerződéshez kapcsolódó adatkezelések 42](#_Toc515536343)

[7.1.5.1 Szerződő magánszemély ügyfelek, partnerek adatainak kezelése 42](#_Toc515536344)

[7.1.5.2 Természetes személy képviselők, kapcsolattartók elérhetőségi adatainak kezelése 43](#_Toc515536345)

[7.1.6 Érintett hozzájárulása alapján történő adatkezelés 44](#_Toc515536346)

[7.1.6.1 Weboldalon történő adatkezelés 44](#_Toc515536347)

[7.1.6.2 Regisztráció a Társaság honlapján 45](#_Toc515536348)

[7.1.6.3 Adatkezelés WEB áruházában 46](#_Toc515536349)

[7.2 Adatfeldolgozás 47](#_Toc515536350)

[7.2.1 Adatfeldolgozói garancianyújtás 48](#_Toc515536351)

[7.3 Adattovábbítás 49](#_Toc515536352)

[8. Adatbiztonság 51](#_Toc515536353)

[8.1 Az adatkezelés biztonsága 51](#_Toc515536354)

[8.2 Hatásvizsgálat módszertana 53](#_Toc515536355)

[8.2.1 Kockázatkezelés 54](#_Toc515536356)

[8.2.2 Adatvédelmi hatásvizsgálat 55](#_Toc515536357)

[8.3 Adatvédelmi incidensek 56](#_Toc515536358)

[8.3.1 Az adatvédelmi incidens kezelése 57](#_Toc515536359)

[8.3.2 Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak 59](#_Toc515536360)

[8.3.3 Az érintett tájékoztatása az adatvédelmi incidensről 60](#_Toc515536361)

[9. Az érintett jogai 61](#_Toc515536362)

[9.1 Átláthatóság és intézkedések 63](#_Toc515536363)

[9.2 Tájékoztatás és a személyes adatokhoz való hozzáférés 63](#_Toc515536364)

[9.2.1 Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik 63](#_Toc515536365)

[9.2.2 Az előzetes tájékoztatás Infotv. 20. § (2) bekezdése szerinti követelményei 64](#_Toc515536366)

[9.2.3 Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg 65](#_Toc515536367)

[9.2.4 Az érintett hozzáférési joga 67](#_Toc515536368)

[9.3 Helyesbítés és törlés 68](#_Toc515536369)

[9.3.1 A helyesbítéshez való jog 68](#_Toc515536370)

[9.3.2 A törléshez való jog („az elfeledtetéshez való jog”) 68](#_Toc515536371)

[9.4 Az adatkezelés korlátozásához való jog 69](#_Toc515536372)

[9.5 Az adathordozhatósághoz való jog 70](#_Toc515536373)

[9.6 A tiltakozáshoz való jog és automatizált döntéshozatal egyedi ügyekben 70](#_Toc515536374)

[9.6.1 A tiltakozáshoz való jog 70](#_Toc515536375)

[9.6.2 Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást 71](#_Toc515536376)

[9.7 Az érintetti kérelmek kezelése 72](#_Toc515536377)

Az Adatkezelési szabályzat változataiban végrehajtott módosítások

Vezetői nyilatkozat

**Hatályba léptetem** jelen **Adatkezelési Szabályzatot**, annak érdekében, hogy a Társaság **alkalmazza** az **Európai Parlament és a Tanács (EU) 2016/679 rendeletét** (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (továbbiakban GDPR).

A rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem.

A **MORGEN-RED Kft**. vezetősége megismerve a GDPR által támasztott kihívásokat, elkötelezett aziránt, hogy a Társaság az adatvédelmi szabályoknak megfeleljen, a szükséges anyagi és személyi erőforrásokat biztosítva, kinevezte a cég belső adatvédelmi felelősét.

Az **Adatkezelési Szabályzat** a GDPR előírásait követve, a **MORGEN-RED Kft.** minden telephelyén és munkaterületén, minden szolgáltatási tevékenységére – **Iró- irodaszer, papíráru, irodatechnikai kisgépek és kellékanyagok forgalmazása** - rögzíti a személyes adatok kezelésére vonatkozó előírásokat, eljárásokat, és egyértelműen meghatározza a kapcsolódó dokumentált információs rendszert.

Az **Adatkezelési Szabályzat** folyamatos karbantartásáért és az abban foglaltak végrehajtásáért az ügyvezető a felelős.

Budapest, 2018. május 25.

………………………

ügyvezető

# Bevezetés

## Az adatkezelési szabályzat célja

Jelen szabályzat célja, hogy a **MORGEN-RED Kft**. munkavállalói vagy egyéb, munkavégzésre irányuló jogviszony alapján foglalkoztatott személyek, illetőleg a Társasággal szerződéses kapcsolatban álló partnerek vagy más harmadik természetes személyek által, meghatározott adatkezelési célból, a Társaság részére átadott személyes adataik kezelése, továbbítása, feldolgozása, tárolása során biztosítva legyen az adatalanyok információs önrendelkezési jogának maradéktalan érvényesülése. Törvényes érdekeik és jogaik védelme, az adatok kezelésének jogszerű célhoz rendelése és a felhasználás alatt mindvégig e jogszerű célhoz kötöttsége.

Az **Adatkezelési Szabályzat** célja továbbá az adatok kezelésének és továbbításának, jogszerűsége, fenntartható legyen azok minősége, és biztosítva legyen az adatok jogosulatlan személyek általi hozzáférhetetlensége. Az adatalanyi minőség - és ezáltal az adatvédelmi szabályoknak történő megfelelés követelménye - a személyes adat jogszerű módon történő megszerzésétől kezdődően, az adott jogviszony létrehozásán keresztül annak fennállása alatt és azt követően is fennáll mindaddig, amíg az adott adatalannyal összefüggésben a személyes adatok végleges és visszafordíthatatlan módon történő törlése - vagy ahol az lehetséges, illetve szükséges, a megsemmisítése - végrehajtásra nem kerül.

Jelen **Adatkezelési Szabályzat** célja továbbá, hogy meghatározza a Társaságnál vezetett adatkezeléssel kapcsolatos nyilvántartások működésének törvényes rendjét, biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak az érvényesülését, valamint hogy a személyes adatok kezelése a jogszabályokban előírtaknak megfelelően történjen.

## Hatály

**Az Adatkezelési Szabályzat hatálya kiterjed a MORGEN-RED Kft. valamennyi munkatársára, szervezeti egységére, továbbá a Társasággal szerződéses jogviszonyban álló valamennyi magánszemélyre, szervezetre, amelynek munkavállalói, vagy alvállalkozói a Társaság által használt rendszerekhez, illetve az azokon tárolt adatokhoz hozzáféréssel rendelkeznek**.

Egyéni vállalkozó, egyéni cég, őstermelő magánszemélyek e szabályzat alkalmazásában természetes személynek minősülnek, így adataik kezelése kapcsán személyes adatkezelés történik.

Jelen Adatkezelési Szabályzat hatálya nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre vonatkozik, beleértve a jogi személy nevét és formáját, valamint a jogi személy elérhetőségére vonatkozó adatokat.

A **MORGEN-RED Kft.** kötelessége, hogy minden érintettnek legyen módja a rájuk vonatkozó elvárások és kötelezettségek megismerésére.

Az **Adatkezelési Szabályzat** hatálya kiterjed a **MORGEN-RED Kft.** használt valamennyi informatikai rendszerre, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi a Társaságnál keletkező, illetve felhasznált személyes adatokat, információkat.

Az **Adatkezelési Szabályzat**ban (és a kapcsolódó szabályzatokban) foglaltak érvényre juttatása érdekében a szabályozás előírásainak betartását minden olyan külső partnerrel kötött szerződésben és megállapodásban kötelezően elő kell írni. Amelynek keretében a külső partner (beleértve annak munkavállalóit, alvállalkozóit, illetve az általa meghívott személyeket) a szabályozás hatálya alá eső helyen munkát végez, szállít vagy a Társaság adataival, adatállományaival, rendszereivel, hálózatával, illetve hálózati eszközeivel bármiféle közvetlen, vagy közvetett kapcsolatban áll.

# Áttekintés az Európai Parlament és a Tanács (EU) 2016/679 rendeletéről

Az Európai Unió hivatalos lapjának 2016. május 4-i számában jelent az új európai adatvédelmi rendelet, amely 2016. május 25-én lépett hatályba és 2 éves felkészülési idő után, 2018. május 25-től kell alkalmazni.

A rendelet pontos megnevezése: Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: Adatvédelmi rendelet, **Rendelet**).

**A rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem**. Továbbá a rendeletet kell alkalmazni akkor is, ha az adatkezelés az Unióban tartózkodó érintettek személyes adatainak kezelésre irányul, akkor is, ha az Unióban az adatkezelő vagy az adatfeldolgozó tevékenységi hellyel nem rendelkezik (ebben az esetben az adatkezelő uniós képviselőt jelöl ki). Utóbbi adatkezelési tevékenységeknek áruknak vagy szolgáltatásoknak az **Unióban tartózkodó érintettek számára történő nyújtásához kell kapcsolódniuk** (akkor is, ha ingyenesek ezek); vagy az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve, hogy az Unió területén belül tanúsított viselkedésükről van szó.

**Az adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli** – ideértve az elektronikus úton tett –, **vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez**.

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

## Alapelvek

1. **Jogszerűség, tisztességes eljárás és átláthatóság**

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

1. **Célhoz kötöttség**

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

1. **Adattakarékosság**

A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.

1. **Pontosság**

A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék, vagy helyesbítsék a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról.

1. **Korlátozott tárolhatóság**

A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor. Az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

1. **Integritás és bizalmas jelleg**

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

1. **Elszámoltathatóság**

Az adatkezelő felelős a fenti alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

## Bizonyítható hozzájárulás

Ha az adatkezelés az érintett hozzájárulásán alapul, az adatkezelőnek kell **tudni bizonyítania, hogy az adatkezelési művelethez az érintett hozzájárult**. Különösen a más ügyben tett írásbeli nyilatkozattal összefüggésben garanciákkal szükséges biztosítani azt, hogy az érintett tisztában legyen azzal a ténnyel, hogy hozzájárulását adta, valamint azzal, hogy ezt milyen mértékben tette. Az adatkezelő előre megfogalmazott hozzájárulási nyilatkozatról gondoskodik, amelyet érthető és könnyen hozzáférhető formában bocsát rendelkezésre, nyelvezetének, pedig **világosnak és egyszerűnek kell lennie**, és nem tartalmazhat tisztességtelen feltételeket. Ahhoz, hogy a hozzájárulás tájékoztatáson alapulónak minősüljön, az érintettnek legalább tisztában kell lennie az **adatkezelő kilétével és a személyes adatok kezelésének céljával**.

A hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett **nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna.**

## Érthető, részletes tájékoztatás, gyors intézkedés

Az adatkezelőnek megfelelő intézkedéseket kell hoznia annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi **tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető** formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban (akár elektronikusan) kell megadni.

Az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen **a kérelem beérkezésétől számított egy hónapon belül tájékoztatja** az érintettet jogai érvényesítésével kapcsolatos intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. Ha az adatkezelő n**em 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 valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.**

Az adatkezelési tájékoztatónak tartalmaznia kell az alábbiakat:

* az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei,
* az . elérhetőségei, ha van ilyen,
* a személyes adatok tervezett kezelésének célja,
* az adatkezelés jogalapja,
* a 6. cikk (1) bekezdésének f) pontján alapuló adatkezelés esetén, az adatkezelő, vagy harmadik fél jogos érdekei,
* adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen,
* adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

## Az érintett jogai

1. **A hozzáférés joga**

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a rendeletben felsorolt információkhoz hozzáférést kapjon.

1. **A helyesbítéshez való jog**

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

1. **A törléshez való jog**

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje meghatározott feltételek esetén.

1. **Az elfeledtetéshez való jog**

Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az 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.

1. **Az adatkezelés korlátozásához való jog**

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

* az érintett **vitatja a személyes adatok pontosságát**, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát,
* az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és e helyett kéri azok felhasználásának korlátozását,
* az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez, vagy védelméhez,
* az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

1. **Az adathordozhatósághoz való jog**

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta.

1. **A tiltakozáshoz való jog**

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is.

1. **Tiltakozás közvetlen üzletszerzés estén**

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

## Az adatkezelő feladatai

1. **Adatkezelési nyilvántartás**

Minden adatkezelő és adatfeldolgozó és – ha van ilyen – az adatkezelő/adatfeldolgozó képviselője a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet. A nyilvántartás-vezetési kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve,

* ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár,
* ha az adatkezelés nem alkalmi jellegű, vagy
* ha az adatkezelés kiterjed a személyes adatok különleges kategóriáinak vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

1. **Az adatkezelés biztonsága**

Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

1. **Az adatvédelmi incidens bejelentése**

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

1. **Adatvédelmi hatásvizsgálat**

Ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

1. **Előzetes konzultáció**

Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelő konzultál a felügyeleti hatósággal.

1. **Az . kijelölése**

Az adatkezelő és az adatfeldolgozó .t jelöl ki minden olyan esetben, amikor:

* az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat,
* az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé,
* az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok különleges kategóriáinak és büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

## Az adattovábbítás általános elve

Olyan személyes adatok továbbítására, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá, vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, e rendelet egyéb rendelkezéseinek betartása mellett, ha az adatkezelő és az adatfeldolgozó a rendelet feltételeinek megfelel.

# Fogalomtár

A használt és a gyakorlatban alkalmazott, az adatvédelem tárgykörébe tartozó kifejezések, meghatározások megfelelnek az **Európai Parlament és a Tanács (EU) 2016/679 rendelet**ében használt kifejezéseknek, és értelmezésük is azonos ezekkel. Az alapvető, valamint a **Szabályzat** készítése során megfogalmazott, a tevékenységek végzése közben használatos fogalmak az alábbiak.

*Adatvédelem*

A személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

*Személyes adat*

Bármely meghatározott, azonosított vagy azonosítható természetes személlyel [érintett] kapcsolatba hozható adat és az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

*Adatalany/érintett*

Bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt –közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

*Különleges adat*

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

*Bűnügyi személyes adat*

A büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

*A szervezet adatvagyona*

A szervezet által kezelt adatok összessége

*Adatkezelés*

Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése. Valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése.

*Adatkezelő*

Az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

*Adatfeldolgozás*

Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől).  
*Adatfeldolgozó*

Az a személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi.

*Szervezeti adatvagyon*

Az adatvagyon fogalmába beleértünk minden külső szervezet számára szolgáltatott, ill. a szervezet saját belső működéséhez szükséges releváns adatot, függetlenül attól, hogy az milyen adathordozón, ill. milyen jelleggel (adatbázis, fájl, papír) áll rendelkezésre.

*Adatkör*

Az azonos működési területekhez tartozó adatok összessége (pl. alkalmazottak adatai, vevők adatai, naplófájlok, stb.)

*Érintett jogai*

Az adatalanyt még az adatkezelés megkezdése előtt, de ezen felül kérésére bármikor egyértelműen tájékoztatni kell az adatkezelés minden részletéről.    Az érintett kérheti adatai helyesbítését, bizonyos esetben törlését is, valamint törvényben meghatározott esetekben tiltakozhat személyes adatai kezelése ellen.

*Az adatkezelés jogalapja*

Főszabály szerint az érintett hozzájárulása vagy törvényben elrendelt kötelező adatkezelés.

*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.

*Biztonsági esemény*

Az a nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amely hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, rendelkezésre állasa, funkcionalitása elvész, megsérül.

*Biztonsági esemény kezelése*

Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.

*Hozzájárulás*

Az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. Különleges adatok esetében szükséges az írásos forma.

*Megfelelő tájékoztatás*

Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

*Tiltakozás*

Az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

*Adatbiztonság*

Az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.

*Az adatkezelés elvei*

A célhoz kötött adatkezelés követelménye (lásd alább), valamint az adatminőség követelménye. Ez utóbbi magában foglalja a pontos, teljes és naprakész adatok igényét, valamint az adatfelvétel és az adatkezelés tisztességes, törvényes mivoltát.

*Célhoz kötött adatkezelés*

Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy  az adatok pontosak, teljesek és - ha az adatkezelés céljára tekintettel szükséges - naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

*Adattovábbítás külföldre*

Személyes adatok továbbítása EGT-n (Európai Gazdasági Térség: az Európai Unió országai, valamint Izland, Norvégia és Liechtenstein) kívüli, harmadik országban adatkezelési tevékenységet folytató adatkezelőhöz.

*Információszabadság*

A közérdekű, valamint közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő alapvető jog, mely elősegíti a közhatalom gyakorlásának demokratikus kontrollját és a közintézmények átláthatóságát (transzparencia).

*Közérdekű adat*

Az állami/önkormányzati feladatot, illetve egyéb közfeladatot ellátó szerv kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret. Függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől (így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat).

*Közérdekből nyilvános adat*

A közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. (pl. a hitelezői érdekek védelme, valamint a piaci forgalom biztonsága érdekében az adatok széles körét minősíti közérdekből nyilvánosnak az ingatlan-nyilvántartásról szóló törvény, a cégtörvény, valamint a számviteli törvény).

*Sztv.*

2000. évi C. törvény a számvitelről

*Pmt.*

2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról

*Szja.*

1995. évi CXVII. Törvény a személyi jövedelemadóról

*Art.*

2017. évi CL. törvény az adózás rendjéről

*Mt.*

2012. évi I. törvény a munka törvénykönyvéről

*Szvtv.*

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

*Avtv.*

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról, a rendszerváltás utáni első adatvédelmi törvény, mely 2011. december 31-ig volt hatályban. 2012. január 1-től hatályon kívül helyezte az Infotv. (lásd alább).

*Infotv.*

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, amelyet az Alaptörvény VI. cikke alapján az Országgyűlés az információs önrendelkezési jog és az információszabadság biztosítása érdekében, az ezen jogok érvényesülését szolgáló alapvető szabályokról, valamint az ellenőrző  hatóságról (NAIH) alkotott. A törvény célja, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák, valamint a közügyek átláthatósága a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon. 2012. január 1-től hatályos.

*NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság*

Az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.

*EDPS (European Data Protection Supervisor)*

A 2004-ben létrejött európai adatvédelmi biztos független intézményként felügyeli az európai intézményekben és uniós szervekben folyó személyes adatok kezelését, emellett az európai adatvédelmi joggyakorlat és jogértelmezés kialakításában is kulcsszerepe van.

*Belső adatvédelmi felelős*

***A***z adatkezelő/adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó azon munkavállaló, aki az adatvédelmi szabályok betartásáért, a személyes adatok védelméért a szervezet nevében felelős.

*Európa Tanács Adatvédelmi Egyezménye*

Az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28-án kelt Egyezmény (az Európa Tanács ún. 108-as Egyezménye). Az első jelentős, az aláíró államokra nézve kötelező erejű nemzetközi jogi dokumentum az adatvédelem terén. Magyarországon kihirdette az 1998. évi VI. törvény, 1998. február 27-én.

*Uniós adatvédelmi irányelv*

Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Az Európai Unió 1995. október 24-én született általános adatvédelmi irányelve, mely – többek között – létrehozta az ún. 29-es Adatvédelmi Munkacsoportot (lásd alább).

*29-es Munkacsoport*

A 95/46/EK irányelv 29. cikkében meghatározott, a tagállamok adatvédelmi biztosaiból, illetve adatvédelmi hatóságainak képviselőiből álló független tanácsadó, véleményező és konzultatív fórum. Állásfoglalásaival és javaslataival segíti az Európai Bizottság munkáját az európai polgárok információs önrendelkezési jogának védelme érdekében.

*Schengen/SIS*

A schengeni térség létrehozása a személyek szabad mozgását lehetővé tevő legfontosabb uniós vívmány. A belső határok eltörléséből és a külső határok megszigorított ellenőrzéséből eredő biztonsági kockázatokat a Schengeni Információs Rendszer (SIS), Európa legnagyobb informatikai rendszere hivatott kezelni, elsősorban a hatékony adatmegosztás eszközével. A tagállamok keresett és eltűnt személyekkel, ellopott vagy elveszett tulajdonnal, beutazási tilalmakkal kapcsolatos adatokat – úgynevezett figyelmeztető jelzéseket – helyeznek el a SIS-ben. Az érintettek SIS-sel kapcsolatos adatvédelmi kéréseikkel (például tájékoztatási vagy helyesbítési kérelem) bármely rendőrkapitánysághoz vagy magyar külképviselethez fordulhatnak, akik ezt továbbítják az ORFK NEBEK SIRENE Irodához. A magyar SIS adatkezelések jogszerűségét a NAIH felügyeli.

*EURODAC: (European Dactyloscopy)*

A 2725/2000/EK rendelet által életre hívott európai ujjnyomat nyilvántartó adatbázis, melynek elsődleges célja a menedékkérők és illegális migránsok beazonosítása.

*OECD irányelvek*

A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) Tanácsa által elfogadott, a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelvei, melyek 1980. szeptember 23-án léptek életbe.

*BCR (Binding Corporate Rules – Kötelező Erejű Vállalati Szabályok)*

A multinacionális társaságok által alkalmazott és a bejegyzés székhelye szerinti EU-tagállam adatvédelmi hatósága által jóváhagyott kötelező magatartási kódex. Ennek értelmében a multinacionális cégcsoport vállalja, hogy a vállalatcsoporton belüli, az EU tagállamok területéről harmadik, nem uniós országba történő adattovábbítás során megfelelő, a cél országban egyébként szokásosnál nagyobb szintű védettséget biztosít az általa továbbított személyes adatoknak.

*ACTA (Anti-Counterfeiting Trade Agreement – Hamisítás elleni kereskedelmi megállapodás)*

Nemzetközi megállapodás, melynek deklarált célja az interneten terjedő kalóztartalmakkal szembeni hatósági fellépés lehetőségének megteremtése. A megállapodás hivatalos előterjesztője Japán volt, a dokumentum 2011 márciusában nyílt meg aláírásra. A megállapodás létrehozására irányuló nemzetközi tárgyalások folyamán az európai adatvédelmi biztos (EDPS) 2010 februárjában kiadott véleményében a dokumentum uniós adatvédelmi szabályokkal való összeegyeztethetőségével kapcsolatban aggályát fejezte ki - az Európai Unió nem csatlakozott hozzá.  
  
*Cloud computing („számítástechnikai felhő", „felhő alapú informatika")*

Számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhő alapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (pl.: Gmail),  vagy az online tárhelyek (pl.: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A  szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni.

*Cookie-k („sütik")*

Rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl.: egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Az Európai Bizottság irányelvei alapján cookie-kat [kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek] csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni. A cookie-k ugyanis számos adatvédelmi aggályt vetnek fel, például a segítségükkel nyomon követhetőek a felhasználó böngészési szokásai.

*Privacy by default*

Olyan adatvédelmi irányzat, melynek lényege, hogy személyes adatok gyűjtésére, kezelésére, illetve feldolgozására csak és kizárólag az adatalany kifejezett kérésére kerülhet sor. Az adatkezelők alapvető, „alapértelmezett” (angolul: by default) hozzáállása az kell, hogy legyen, hogy minden körülmények között figyelembe veszik az adatvédelmi szempontokat és ezeknek megfelelően járnak el az adatkezelési műveletek során.

*Privacy by design*

Kanadában, az 1990-es években kialakult adatvédelmi irányzat. Lényege, hogy az adatvédelmi szempontoknak megfelelő gyakorlat nem merülhet ki a hatályos szabályozásnak való formális megfelelésben. Az adott szervezet alapvető működési elve az adatvédelmi szempontoknak való megfelelés, ezért működését, struktúráját ezek maximális figyelembevételével alakítja ki, az adatvédelmi szempontokat már az egyes működési fázisok megtervezésekor beépíti és így biztosítja az adatvédelem teljes körű érvényesülését. Rokon területe a „privacy by default” megközelítésnek.

*Munkahely*

A „munkahely” fogalma alatt valamennyi, a felhasználók által használt végponti készüléket és mobil adathordozót kell érteni.

*Archiválás*

Az archiválás a Szervezeti alaptevékenység szempontjából lényeges azon információk és dokumentumok tárolásának célját szolgálja, amelyekre a folyamatban lévő feladatok teljesítéséhez már nincs szükség, de jogi követelmények miatt vagy más célokra bizonyos időpontig (tárolási időtartam) megőrzendők.

*Archivált adatok*

„Archivált adatok” elnevezéssel jelöljük azokat az információkat és dokumentumokat, amelyek archívumban kerültek elhelyezésre. Az archivált adatokat időállóan és igazolhatóan, alkalmas technológiák segítségével kell tárolni, pl. elektronikus, mágneses, optikai vagy kinyomtatott formában.

*Archiválási rendszer*

Az archiválási rendszer alatt az archiváláshoz felhasznált, hardver- és szoftver-elemekből álló technikai rendszert értjük.

*Megőrzési időtartam*

A megőrzési időtartam alatt azon időtartamot értjük, amely azzal a nappal záródik le, amelyen a törvényi vagy egyéb, a megőrzésre vonatkozó követelmény véget ér.

*Backup*

Backup (adatmentés) alatt az információknak az esetleges adatvesztéssel szembeni védelmét szolgáló kiegészítő tároló közegen történő mentését értjük. Ily módon biztosítja a backup az információk rendelkezésre állását és integritását.

# Kapcsolódó külső és belső szabályok

Az **Adatkezelési Szabályzat** a **MORGEN-RED Kft.** minden szolgáltatási tevékenységére rögzíti az adatkezeléssel kapcsolatos teendőket.

* **A szabályzat kialakítása során figyelembe vett főbb jogszabályok, ajánlások:**

**Európai Parlament és a Tanács (EU) 2016/679 rendelete** (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról

**2011. évi CXII. t**örvény az információs önrendelkezési jogról és az információszabadságról

**2012. évi I.** törvény a munka törvénykönyvéről

**2013. évi V.** törvény a polgári törvénykönyvről

**1995. évi CXVII.** törvény a személyi jövedelemadóról

**2017. évi CL.** törvény az adózás rendjéről

**1997. évi CLV.** törvény a fogyasztóvédelemről

**2000. évi C.** törvény a számvitelről

**2001. évi CVIII.** törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

**2003. évi C.** törvény az elektronikus hírközlésről

**2008. évi XLVIII.** törvény a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól

**1997. évi LXXX. t**örvény a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről

**2005. évi CXXXIII. t**örvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

**2017. évi LIII.** törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról

**2008. évi XLVII.** törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról

**2005. évi XC.** törvényaz elektronikus információszabadságról

**2003. évi C.** törvény az elektronikus hírközlésről (kifejezetten a 155.§)

**16/2011. sz. vélemény** a viselkedésalapú online reklám bevált gyakorlatára vonatkozó EASA/IAB-ajánlásról

**Az informatikai biztonság irányításának követelményrendszere** (IBIK) 0.91 verzió 2004

**HAIH ajánlások**:<https://www.naih.hu/ajanlasok.html>

**29-Adatvédelmi Munkacsoport dokumentumai:** <https://naih.hu/29--adatvedelmi-munkacsoport-dokumentumai.html>

* **A kapcsolódó belső szabályzatok, előírások, eljárások:**

Minőségirányítási kézikönyv (ISO 9001:2015)

Az **Adatvédelmi Szabályzat**ban leírtak a **MORGEN-RED Kft.** minden olyan munkatársára érvényesek és kötelezőek, akik az adatkezeléssel kapcsolatos folyamatokban, tevékenységekben bármi módon részt vesznek.

# Felelősségi körök

## Szervezeti felépítés

A Társaságnak az Adatkezelési szabályzatban foglalt előírások hatékony működtetéséhez megfelelő létszámú, jól felkészült munkatárs áll rendelkezésre. Az egyes funkciókat betöltő munkatársak feladatait a munkaköri leírások tartalmazzák részletesen. Mivel az **Adatkezelési Szabályzat** hatálya kiterjed a **MORGEN-RED Kft.** valamennyi **munkatársára**, és a Társaság által használt valamennyi **informatikai rendszerre**, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi a Társaságnál keletkező, illetve felhasznált személyes adatokat, információkat a Társaság vezetőjének feladata, hogy az érintetteknek legyen módjuk a rájuk vonatkozó elvárások és kötelezettségek megismerésére.

A **MORGEN-RED Kft.** szervezeti felépítése:

**Szervezeti ÁBRA**

A **MORGEN-RED Kft.** ügyvezetője felelős azért, hogy:

* A személyes adatoknak bármilyen jellegű kezelése tekintetében az adatkezeléssel kapcsolatos hatásköröket és felelősségét egyértelműen meghatározza, szabályozza.
* Megfelelő és hatékony intézkedéseket hajtson végre, valamint képes legyen igazolni azt, hogy a Társaság adatkezelési tevékenységei a **Rendelet**nek megfelelnek, és az alkalmazott intézkedések hatékonysága is a **Rendelet** által előírt szintű. Az intézkedéseket az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell meghozni.
* A Társaság olyan adatfeldolgozókat vegyen igénybe, amelyek megfelelő garanciákat nyújtanak – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – arra vonatkozóan, hogy az a rendelet követelményeinek teljesülését biztosító technikai és szervezési intézkedéseket végrehajtják, ideértve az adatkezelés biztonságát is.
* A **Rendelet** előírásai szerint szükség szerint Képviselőt jelöljön ki. A Képviselő az adatkezelő vagy az adatfeldolgozó nevében jár el, és e minőségében bármelyik felügyeleti hatóság megkeresheti.

A **MORGEN-RED Kft**. ügyvezetője nevezi ki a belső adatvédelmi felelőst, aki a Társaságon belül, közvetlenül annak vezetőjének felügyelete alá tartozó azon munkavállaló, aki az adatvédelmi szabályok betartásáért, a személyes adatok védelméért a szervezet nevében felelős.

A belső adatvédelmi felelős a következő feladatokat látja el:

* Tájékoztat és szakmai tanácsot ad a Társaság vezetősége, továbbá az adatkezelést végző alkalmazottak részére a **Rendelet**, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban.
* Ellenőrzi a **Rendelet**nek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá a Társaság személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is.
* Kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését.
* Együttműködik a felügyeleti hatósággal.
* Az adatkezeléssel összefüggő ügyekben – ideértve a 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

A belső adatvédelmi felelős az adatkezelési előírások betartatásához, érvényesítéséhez, a leírt szabályozások végrehajtatásához minden jogkörrel és eszközzel rendelkezik, akinek folyamatos beszámolási kötelezettsége van a vezető felé a **MORGEN-RED Kft.** adatkezelési rendszerének működtetésével, folyamatos fejlesztésével és az alkalmazható, előírt követelmények, feladatok teljesítésével kapcsolatban.

## Képzés

A Társaság vezetősége meghatározta a szükséges felkészültséget minden dolgozó esetében, akik a felügyelete alatt olyan munkát végeznek, amely hatással van a szervezet adatkezelési tevékenységére. A vezetőség feladata, hogy biztosítsa az adatkezelési műveletekben vevő személyzet folyamatos tudatosság-növelését és képzését ezért, hogy a munkatársak felkészültek legyenek megfelelő oktatás, képzés vagy gyakorlat alapján.

A vezetőség folyamatosan kiértékeli az elvégzett tevékenységek eredményességét, biztosítja, hogy a munkatársak tudatában legyenek a **MORGEN-RED Kft.** adatkezelési/adatfeldolgozási tevékenységében betöltött szerepüknek és annak fontosságának.

A belső adatvédelmi felelős feladata, hogy felmérje a képzési szükségleteket és megszervezze az adatkezeléssel kapcsolatos külső és belső oktatásokat, képzéseket, és ezekről a megfelelő feljegyzéseket (Oktatási tematika, Képzési napló, stb.) megőrizze.

A belső adatvédelmi felelős legalább évente egyszer képzést tart a Társaság minden munkatársa számára, ahol ismerteti a **Rendeletet** és jelen **Adatkezelési szabályzat** előírásait. A belső adatvédelmi felelős feladata a mindennapi munkája során a munkatársak folyamatos tudatosság-növelése és folyamatos továbbképzése, a vállalati adatvédelmi szabályok fontosságának előtérbe helyezése, bemutatása.

A belső adatvédelmi felelős kompetenciája a személyes adatokba állandó jelleggel vagy rendszeresen betekintő személyzetnek nyújtandó megfelelő személyre szóló adatvédelmi továbbképzés megtartása, valamint közös képzési és csereprogramok (pl. felügyeleti hatóságok között, valamint adott esetben harmadik országok felügyeleti hatóságaival vagy nemzetközi szervezetekkel) támogatása.

# Felülvizsgálat, ellenőrzés, szakmai kapcsolattartás

## Felülvizsgálat, ellenőrzés

**A MORGEN-RED Kft**. tervezett időközönként, legalább évente egyszer, átfogó, belső helyszíni adatkezelési felülvizsgálatokat végez, hogy információkat kapjon arról, a Társaság adatkezelési tevékenysége megfelel a **Rendelet** és jelen **Adatkezelési Szabályzat** rendelkezéseinek, előírásainak.

A belső adatkezelési felülvizsgálatokat a ügyvezető rendeli el, és a felülvizsgálatot az általa kijelölt, megfelelő szakmai tudással, okirattal rendelkező munkatársak, és/vagy külső szakértők végzik el. Úgy kell kiválasztani az auditorokat és végrehajtani az auditokat, hogy biztosítva legyen az audit folyamat objektivitása és pártatlansága. Az felülvizsgálatok elvégzésének alapvető módszere az **Adatkezelési Szabályzat**, a vonatkozó jogszabályok, belső dokumentumok előírásainak, követelményeinek összevetése a tényhelyzettel majd az eltéréseke rögzítése.

Az adatkezelési felülvizsgálat során az auditor ellenőrzi az a **Rendelet**nek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá a Társaság személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint áttekinti az érintettek jogainak védelmét szolgáló korrekciós intézkedéseket biztosító mechanizmusokat, az incidensek kezelésére vonatkozó intézkedéseket, és a hatásvizsgálatok eredményét is.

## Szakmai kapcsolattartás

A **MORGEN-RED Kft.** ügyvezetője kinevezte adatkezeléssel összefüggő ügyekben Társaság Kapcsolattartóját.

**A Kapcsolattartó neve: Domiter Zoltánné**

**A Kapcsolattartó elérhetősége: domiter.rita@morgenred.hu**

A Kapcsolattartó az adatkezeléssel összefüggő ügyekben (pl. incidens bejelentése, stb.) kapcsolattartó pontként szolgál a felügyeleti hatóság (NAIH) felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytathat vele.

# Személyes adatok kezelése, nyilvántartás

## Adatkezelés

**A MORGEN-RED Kft. vezetője felelős** azért,hogy a Társaság az adatkezelési tevékenységét úgy végzi, hogy az feleljen meg a **Rendelet**nek, amely szabályozza a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását, és biztosítja az érintettek számára a jogi garanciákat.

### A személyes adatok kezelésére vonatkozó elvek

**A MORGEN-RED Kft. vezetője felelős** azért,hogy a Társaság az adatkezelési tevékenységét úgy végzi, hogy betartja a személyes adatok kezelésére vonatkozó elveket, és képes e megfelelés igazolására **(„elszámoltathatóság”**).

A **MORGEN-RED Kft.** a személyes adatok;

* kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („**jogszerűség, tisztességes eljárás és átláthatóság**”),
* gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („**célhoz kötöttség**”),
* az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk **(„adattakarékosság”**),
* pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék **(„pontosság**”),
* tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a **Rendelet** 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából. Tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor; az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („**korlátozott tárolhatóság**”),
* kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve **(„integritás és bizalmas jelleg**”).

### Az adatkezelés jogszerűsége

A **MORGEN-RED Kft.** vezetője felelős azért, hogy a Társaság az adatkezelési tevékenységét úgy végzi a **Rendelet** 6. cikk szerint, hogy a személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

* az érintett **hozzájárulását** adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
* az adatkezelés olyan **szerződés teljesítéséhez** szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
* az adatkezelés az adatkezelőre vonatkozó **jogi kötelezettség** teljesítéséhez szükséges;
* az adatkezelés az érintett vagy egy másik természetes személy **létfontosságú érdekeinek védelme** miatt szükséges;
* az **adatkezelés közérdekű** vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
* az adatkezelés **az adatkezelő vagy egy harmadik fél jogos érdekeinek** érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

### Munkavállalók adatkezelése

**A MORGEN-RED Kft. munkavállalónak, mint érintett természetes személyre vonatkozó személyes adatainak kezeléséért a belső adatvédelmi felelős a felelős. A Társaság vállalja, hogy a munkaviszonyhoz kapcsolódóan adatfeldolgozók részére átadott adatok és a folytatott adatkezelési műveletekre vonatkozóan az adatfeldolgozókkal betartatja a Rendelet előírásait és a NAIH** tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről dokumentumot.

A munkavállalók személyi **okmányait, iratait a Társaság nem másolja, fénymásolja, a másolatokat így nem tárolja** elkerülve a készletező adatkezelést. A munkavállalóktól kizárólag olyan adatok kérhetők és tarthatók nyilván, valamint olyan munkaköri orvosi alkalmassági vizsgálatok végezhetők, amelyek munkaviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve a szociális-jóléti juttatások biztosításához szükségesek és a munkavállaló személyhez fűződő jogait nem sértik. Az Mt. rendelkezései szerint a munkavállaló személyiségi joga akkor korlátozható, ha a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. A személyiségi jog korlátozásának módjáról, feltételeiről és várható tartamáról a munkavállalót előzetesen tájékoztatni kell.

Az egyes munkáltatói tevékenységekben a munkavállalók személyes adatai esetileg **különböző jogalapok alapján** kerülnek kezelésre, így: **jogi kötelezettség,** **munkaszerződés teljesítése**, **munkáltatói jogos érdek**, illetve **érintett hozzájárulása** alapján.

A **MORGEN-RED Kft**., az adatkezelő vezetősége megfelelő intézkedéseket hozott annak érdekében, elősegítse a **Rendelet**ben szereplő összes **érintett személy jogai**nak – a visszavonás jogának is - **gyakorlását**, melynek részletes leírása jelen szabályzat 9. fejezetében található.

#### Adatkezelés az érintett hozzájárulása alapján

A **hozzájáruláson alapuló adatkezelés** esetén az érintett munkavállaló **írásbeli hozzájárulását adja** a személyes adatai kezeléséhez. A jelenlegi joggyakorlat alapján munkaviszonyban a munkavállaló hozzájárulása nem lehet önkéntes, mert egyfajta egyensúlytalanság, hatalmi viszony áll fent a munkáltató javára. Egy hozzájárulás egy adatkezelési cél érdekében végzett adatkezeléshez való hozzájárulást jelenti. Több adatkezelési cél esetén több önkéntes, egyértelmű érintetti hozzájárulás szükséges.

**Az érintett munkavállaló írásbeli hozzájárulást hozzájárulási jognyilatkozat aláírásával ad, amelyet a belső adatvédelmi felelősének kell a továbbiakban megfelelően tárolnia, kezelnie, szükség szerint nyilvántartásba vennie.**

#### Adatkezelés jogi kötelezettség teljesítése érdekében

Jogi kötelezettség teljesítése jogalapon alapuló adatkezelés az érintett hozzájárulásától független, mivel az adatkezelést jogszabály határozta meg, így ekkor az adatkezelés célja a jogi előírásoknak való megfelelés. Az adatkezelés kötelező jellegétől függetlenül az érintett magánszeméllyel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés kötelező és nem kerülhető el. **Az érintett személy számára a belső adatvédelmi felelős feladata az adatkezelés megkezdése előtt egyértelmű és részletes tájékoztatást adni az adatai kezelésével kapcsolatos minden jelentős tényről.**

A tájékoztatásnak ki kell terjednie az adatkezelés céljára és jogalapjára, az érintett magánszemélynek adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire, az adatkezelő és az adatfeldolgozó személyére, az adatkezelés időtartamára, jogi kötelezettség teljesítésre, mint jogalapra, illetve az azokról a személyekről való tájékoztatásra, hogy kik férhetnek hozzá, kik ismerhetik meg az adatokat. Kötelező adatkezelés esetén a tájékoztatás megtörténhet az előbbi információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is. Az érintett magánszemélyt tájékoztatni kell a személyes adatai adatfeldolgozó részére történő továbbításáról is.

##### Adatkezelés munkaviszony létesítése, teljesítése és kapcsolódó nyilvántartási kötelezettségeknek való megfelelés érdekében

A munkavállalóktól kizárólag olyan személyes adatok szerezhetők be és tarthatók nyilván, amelyek munkaviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve az adó- és társadalombiztosítási kötelezettségek teljesítéséhez szükségesek, s a munkavállaló személyhez fűződő jogait nem sértik.

**Belső adatvédelmi felelős feladata munkaviszony létesítése (illetve meglévő munkaviszony teljesítése) esetén a** [**https://www.gdpreg.hu**](https://www.gdpreg.hu) **alkalmazásban generált hozzájárulási jognyilatkozatot a munkavállalóval aláíratni, azt a továbbiakban megfelelően tárolnia, kezelnie, szükség szerint nyilvántartásba vennie.**

A <https://www.gdpreg.hu> alkalmazásban a munkaviszonyhoz kapcsolódó adatkezelések a különböző személyes adatok jogszabályokban meghatározott eltérő megőrzési ideje szerinti bontásban kerültek csoportosításra (pl. családi pótlék, munkaviszony megszüntetése, stb.)

**Az adatkezelés célja:** munkaviszony létesítése, teljesítése és kapcsolódó nyilvántartási kötelezettségeknek való megfelelés

**Az adatkezelés jogalapja:** jogi kötelezettség teljesítése

**Kezelt adatok lehetnek:** név, születési név, születési hely/idő, anyja neve, lakcím, állampolgárság, adóazonosító jel, TAJ szám, személyi igazolvány szám, lakcímet igazoló hatósági igazolvány szám, bankszámlaszám, munkaviszony kezdetének és végének napja, munkakör megnevezése, munkabérének összege, a bérfizetéssel, egyéb juttatásaival kapcsolatos adatok, a munkavállaló munkabéréből jogerős határozat vagy jogszabály, illetve írásbeli hozzájárulása alapján levonandó tartozás, a munkaviszony megszűnésének módja, indokai, munkakörtől függően erkölcsi bizonyítvány, a munkaköri alkalmassági vizsgálatok összegzése, magánnyugdíj pénztári és önkéntes kölcsönös biztosító pénztári tagság esetén a pénztár megnevezése, azonosító száma és a munkavállaló tagsági száma, külföldi munkavállaló esetén útlevélszám/munkavállalási jogosultságot igazoló dokumentum megnevezése és száma, munkahelyi baleseti jegyzőkönyveiben rögzített adatok, pályakezdő, családi pótlékra jogosult gyerekek száma, legmagasabb végzettség

**Az adatok felelősei és címzettjei**: ügyvezető, irodavezető és az adatfeldolgozó: Eden&LLoyd Kft. (Halmai Gábor)

**Az adatok tárolásának időtartama**: a jogi kötelezettséget előíró jogszabályokban meghatározott időtartam

**Adattárolás helye, módja**: papír alapon a munkavállaló munkaügyi dossziéjában, illetve elektronikusan Iwise vállalatirányítási rendszerben.

**A belső adatvédelmi felelős felelőssége kezelni, és folyamatosan aktualizálni a** [**https://www.gdpreg.hu**](https://www.gdpreg.hu) **alkalmazásban a „Személyi törzsadatok: munkavállalók (tetszőleges) adatainak importálása” menüponthoz kapcsolódó adatokat.**

Betegségre, szociális védelemre és szakszervezeti tagságára vonatkozó adatokat (munkaidő kedvezmény, stb.) a Társaság csak a Mt.-ben meghatározott jog, vagy kötelezettség teljesítése céljából kezel.

##### Alkalmassági vizsgálatokhoz kapcsolódó adatkezelés

A Társaságnál a **munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály, mint jogi kötelezettséget előíró szabály határoz meg** (mint például Mt. által előírt alkalmassági vizsgálat), illetve lehetőség van olyan alkalmassági és egyéb vizsgálatok elvégzésére, amelyet nem munkaviszonyra vonatkozó szabály ír elő, de **munkaviszonyban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.**

Minden vizsgálat előtt a belső adatvédelmi felelős feladata, hogy érthetően és részletesen tájékoztatja a munkavállalókat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatja a munkavállalókat a jogszabály címéről és a pontos jogszabályhelyről is.

A kizárólag munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében csak akkor alkalmazható a munkavállaló pszichológiai állapotának vagy személyiségjegyének elemzésére alkalmas tesztlap, ha az nem egyedileg egy munkavállalóra vonatkozik, hanem a munkavállalók egy csoportjára, s ha az elemzés során megállapításra került adatok nem köthetők az egyes konkrét munkavállalóhoz, tehát hiányzik a személyes adat fogalmának alapvető eleme: a beazonosíthatóság.

A munkaalkalmasságra, a munkaköri feladat ellátásának való megfelelőségre, felkészültség ellenőrzésére irányuló vizsgálatokat, kérdéssorokat, teszteket a **munkáltató mind a munkaviszony létesítése előtt, mind a munkaviszony fennállása alatt alkalmazhat**.

**A vizsgálat eredményét a vizsgálatot végző szakember és az érintett munkavállaló ismerheti meg.** A munkáltató vezetője, munkáltatói jogkör gyakorlója számára csak az az információ adható át, hogy a vizsgált személy **a munkára alkalmas-e vagy sem**, illetve milyen feltételek biztosítandók ehhez. A fentieken felüli vizsgálati eredményt, illetve annak részletes dokumentáltságát a munkáltató nem ismerheti meg. Nem kezelhető a munkáltató részéről semmilyen szakmai tesztlapra, kérdéssorra adott válasz és az azokból levonható következtetés.

A Társaság a munkaviszony létesítése előtt és fennállása alatt kérheti a munkavállalótól /álláspályázótól/ feddhetetlen előéletének az igazolását, mely célra az ún. Erkölcsi Bizonyítvány bemutatása szolgál, de nem kéri, hogy az érintettek hatósági erkölcsi bizonyítvány helyett bűnügyi nyilvántartó szervtől szerezzenek be nemleges igazolást.

**Az adatkezelés célja:** jogi kötelezettséget előíró szabály teljesítése

**Az adatkezelés jogalapja:** jogi kötelezettség teljesítése

**Kezelt adatok lehetnek:** a munkaköri alkalmasság ténye vagy hiánya és az ehhez szükséges feltételek

**Az adatok felelősei és címzettjei**: ügyvezető, irodavezető

**Az adatkezelés időtartama**: munkaszerződés/jogi kötelezettséget előíró jogszabály, a munkaviszony fennállásának időtartama, illetve azon túl a munkaügyi követelések elévülési ideje, amennyiben a vizsgálatnak van vonatkozása a követeléshez

**Adattárolás helye, módja**: papír alapon a munkavállaló munkaügyi dossziéjában.

#### Szerződéshez kapcsolódó adatkezelések

A **Rendelet** szerint lehetőség van személyes adatok kezelésére, ha az adatkezelés olyan szerződés (munkaszerződés) teljesítéséhez szükséges, amelyben az érintett magánszemély az egyik fél, vagy az adatkezelés, adatfelvétel a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

#### Adatkezelés munkáltatói jogos érdek alapján

A Társaságnak a munkavállalóval fennálló munkaviszonya alatt, illetve azt megelőzően és azt követően is fűződhet érdeke személyes adatok kezeléséhez. Az esetek jelentős részében az adatkezelés jogalapja nem az egyébként kapcsolódó jogi kötelezettségek teljesítése, hanem a **munkáltatói jogos érdeken** alapuló adatkezelés, **amelyhez egy a** [**https://www.gdpreg.hu**](https://www.gdpreg.hu) **alkalmazásban elkészített Érdekmérlegelési teszt szükséges.**

A jogos munkáltatói érdek alapján történő adatkezelések végrehajtásáért, nyilvántartásáért és ellenőrzéséért a belső adatvédelmi felelős a felelős, melynek részletes szabályozását a következő 7.1.3.5.-7.1.3.13. fejezet tartalmazza.

A **MORGEN-RED Kft.** vezetősége, mint munkáltató az adatkezelés célját minden esetben világosan és egyértelműen határozza meg. A munkavállalóktól kért adatok köre, és az alkalmazott vizsgálatok csak olyan esetekre vonatkozhatnak, amikor azok lényeges tájékoztatást adhatnak a munkaviszony létesítése, fenntartása, megszüntetése szempontjából. A Társaság vezetősége figyel a szükségesség-arányosság elvére, hogy az alkalmazott eszköz alkalmas legyen az adatkezelési cél elérésére, csak szükséges mértékű adatkezeléssel járjon, és ellenőrzés csak a munkavégzéssel összefüggésben történjen, és soha nem irányuljon a munkavállalók emberi méltóságának a sérelmére, így a munkavállalók megfélemlítésére, megalázására, zaklatására, zavarására.

A Társaság vezetősége különösen figyel arra, hogy a munkavállalókat a munkahelyen is megilleti a magánélethez való jog, amelyeknek tipikus színterei: ebédlő, öltöző, pihenő helyiség, mosdók.

**A jogos érdek jogalap szerinti adatkezelések a következők:**

* álláspályázatok adatkezelése,
* munkáltatói e-mail cím/fiók használata,
* munkahelyi internet és wifi használata,
* munkáltatói számítógép használata,
* munkáltatói mobiltelefon, telefon használata.

##### Álláspályázatok adatkezelése

A **MORGEN-RED Kft.** vezetősége figyel arra, hogy álláspályázat meghirdetése esetén **előzetes tájékoztatás keretén belül biztosítsa saját adatkezelő voltának és elérhetőségének a megismerhetőségét**, és **csak olyan személyes adatok megismerhetőségére tart igényt, amelyek lényegesek az adott munkakörrel kapcsolatban**. A Társaság megismerheti az adott állásra pályázó közösségi oldalakon közzétett nyilvános, a munkavégzés szempontjából lényeges személyes adatait, de erről a körülményről előzetes tájékoztatást nyújt a pályázó számára a belső adatvédelmi felelős, ugyanakkor a pályázó közösségi oldalával kapcsolatban személyes adatot nem ment le, nem tárol, nem továbbít.

**Az adatkezelés célja:** munkaviszony létesítéséhez szükséges adott munkakörhöz kapcsolódó lényeges adatok megismerése

**Az adatkezelés jogalapja:** munkáltatói jogos érdek

**Kezelt adatok lehetnek:** a munkaköri alkalmasság ténye vagy hiánya és az ehhez szükséges feltételek

**Az adatok felelősei és címzettjei**: ügyvezető

**Az adatkezelés időtartama**: sikeres pályázat esetén a munkaügyi szabályok szerinti időtartamig, sikertelen pályázat esetén a pályázatról való döntést követő 5. napig, amikor a sikertelen pályázati anyagok teljes mértékben törlésre kerülnek, amelyről a sikertelen pályázók értesítést kapnak

**Adattárolás helye, módja**: papír alapon a felvételi dossziékban, elektronikusan a munkáltató által használt e-mail levelező rendszerben.

##### Munkáltatói e-mail cím/fiók használata

A **MORGEN-RED Kft.** vezetősége **tiltja az általa biztosított e-mail fiókban a magáncélú levelezést,** azt a munkavállaló **csak munkavégzésére használhatja fel. Az e-mail fiók tartalmáról biztonsági másolat nem készül, nem kerül sor személyes adatok kezelésére.** A Társaság vezetősége a szervezet üzleti titkainak védelme, üzleti tevékenységének, partner kapcsolatainak, és piaci részesedésének titokban tartása, illetve a munkavégzés ellenőrzése céljából ellenőrizheti a munkavállalók munkáltató által biztosított e-mail fiókjának tartalmát, az abban végbemenő kimenő és beérkező adatforgalmat. A kapcsolódó adatkezelés jogalapja: munkáltató jogos érdeke, ezért a Társaság elvégezte az Érdekmérlegelési tesztet, melyet minden munkavállalóval megismertet.

**A belső adatvédelmi felelős felelőssége, hogy felhívja minden munkavállaló figyelmét, hogy amennyiben a tiltás ellenére magáncélra is használja az e-mail fiókot, úgy esetlegesen védett személyes adataihoz, vagy az abból származó következtetésekhez való hozzáférés kockázatának teszi ki magát, valamint tájékoztat minden munkavállalót arról, hogy a munkahelyi levelezés megfigyelése nem jogsértő munkáltató részéről, ebben a tárgyban az Emberi Jogok Európai Bíróságának is született ítélete.**

Az ügyvezető feladata a munkavállalók e-mail szúrópróbaszerű **dokumentált ellenőrzése**, amelynek **során betartja a fokozatosság elvét**. Az e-mail fiók ellenőrzésének első lépése az e-mail címzettjének/küldőjének és a levél tárgyának az ellenőrzése. Amennyiben ennyiből megállapítható, hogy a levél tartalmának megnyitása személyes adathoz való hozzáférést eredményezhet, úgy a belső adatvédelmi felelős nem nyitja meg a levelet. Amennyiben nem valószínűsíthető a személyes adathoz való hozzáférés, úgy munkáltató jogosult az e-mailt megnyitni és áttanulmányozni, különös tekintettel a kapcsolódó fájlokra. Amennyiben a belső adatvédelmi felelős mégis személyes adatra bukkan, úgy azt nem jogosult megismerni. Az ellenőrzés során, ha a belső adatvédelmi felelős talál nem a munkavégzéshez kapcsolódó e-mail, akkor annak törlésére felszólítja a munkavállalót, aki a levél törlését haladéktalanul köteles elvégezni. Az e-mail fiók ellenőrzése során minden esetben **biztosított a munkavállaló jelenléte**, amennyiben ez mégsem lehetséges (pl. betegség, baleset, szabadság), úgy csak tanú jelenlétében végezhető el az ellenőrzés.

Az ügyvezető feladata tájékoztatni ellenőrzés előtt a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról, amelyek:

* az ellenőrzés célja (pl. annak ellenőrzése, hogy nem került-e ki ügyfél adat),
* eljárási szabályok, lépések: munkavállaló tájékoztatása ellenőrzésről, e-mail fiókba való munkavállalói belépés, ellenőrző személy szemrevételezi az e-mailek címzettjeit, tárgymezőket, egyeztetés munkavállalóval, hogy melyek a személyes adatokkal érintett levelek, kötetlen formátumú ellenőrzési jegyzőkönyv megírása, aláírása),
* munkavállaló tájékoztatása a jogorvoslati jogokról.

##### Munkahelyi internet és wifi használat

A **MORGEN-RED Kft.** vezetőségedöntése alapján minden munkavállaló **csak a munkavégzésével kapcsolatban használhatja a Társaság által biztosított wifi hálózat elérését, illetve csak a munkavégzéssel kapcsolatos honlapok megtekintésére van lehetőség és tiltja a munkaidőben történő magán célú internet használatot.** A kapcsolódó adatkezelés jogalapja: munkáltató jogos érdeke, ezért a Társaság elvégezte az Érdekmérlegelési tesztet, melyet minden munkavállalóval megismertet, ugyanakkor a munkáltatói tiltás miatt itt **nem kerül sor személyes adatok kezelésére.**

A Társaság nem rögzíti a munkavállalók által meglátogatott honlapok elérhetőségét és egyéb internet használatból levonható következtetéseket, de alkalomszerűen azonnali megtekintéssel az ügyvezető ellenőrizheti, hogy a munkavállaló milyen honlapon tartózkodik. Az ő felelőssége, hogy felhívja a munkavállalók figyelmét, hogy amennyiben a tiltás ellenére valaki magáncélra (is) használja a wifi hálózatot/internetet, úgy annak munkaügyi következményei lehetnek a munkavállaló számára, illetve munkáltató akaratán kívül hozzáférhet személyes adatokhoz.

A Társaság informatikai rendszerének védelme érdekében az ügyvezető feladata szúrópróbaszerűen dokumentáltan **ellenőrizni az internet és wifi használatával kapcsolatos szabályok betartását**, biztosítva az érintett munkavállaló jelenlét, mivel az internet használat ellenőrzése a munkavállaló jelenléte nélkül kizárt. Az ellenőrzés során a belső adatvédelmi felelős betartva a fokozatosság elvét első lépésként az ellenőrzés időpontjában aktuálisan megnyitott honlapot tekinti meg. Amennyiben ennyiből megállapítható, hogy a munkavállaló nem tiltott oldalt tekint meg, úgy az ellenőrzés le is zárult. Amennyiben nem valószínűsíthető a személyes adathoz való hozzáférés, úgy munkáltató folytathatja az ellenőrzést.

Az ügyvezető feladata tájékoztatni ellenőrzés előtt a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról, amelyek:

* az ellenőrzés célja: (pl. annak ellenőrzése, hogy nincs-e tiltott oldal megtekintés)
* eljárási szabályok, lépések: munkavállaló tájékoztatása ellenőrzésről, monitor megtekintése, egyeztetés munkavállalóval, hogy szükséges-e a munkájához a megtekintés alatt álló weboldal, kötetlen formátumú ellenőrzési jegyzőkönyv megírása, aláírása)
* munkavállaló tájékoztatása a jogorvoslati jogokról.

##### Munkahelyi számítógép használata

A **MORGEN-RED Kft.** vezetőségedöntése alapján minden munkavállaló **csak a munkavégzésével kapcsolatban használhatja a Társaság által biztosított számítógépet** (tablet, laptop, stb.), **tiltja az általa biztosított eszközökön a magánélethez kapcsolódó tevékenységek végzését, személyes adatok kezelését, tárolását.** A kapcsolódó adatkezelés jogalapja: munkáltató jogos érdeke, ezért a Társaság elvégezte az Érdekmérlegelési tesztet, melyet minden munkavállalóval megismertet, ugyanakkor a munkáltatói tiltás miatt itt **nem kerül sor személyes adatok kezelésére.**

A **MORGEN-RED Kft.** üzleti titkainak védelme, üzleti tevékenységének titokban tartása, illetve a munkavégzés ellenőrzése céljából az ügyvezető **ellenőrizheti** a munkavállalók a Társaság által **biztosított számítógépen folytatott munkavállalói tevékenységeket**, az eszköz memóriáját, az eszközre és a hozzá csatlakoztatott eszközre vonatkozó biztonsági előírások betartását. Az ő felelőssége, hogy felhívja a munkavállalók figyelmét, hogy amennyiben a tiltás ellenére magáncélra is használja a munkavállaló a biztosított technikai eszközöket, úgy esetlegesen védett személyes adataihoz, vagy az abból származó következtetésekhez való hozzáférés kockázatának teszi ki magát.

Az ügyvezető feladata szúrópróbaszerűen dokumentáltan **ellenőrizni a munkahelyi számítógép használatával kapcsolatos szabályok betartását**, biztosítva az érintett munkavállaló jelenlét, amennyiben ez mégsem lehetséges (pl. betegség, baleset, szabadság), úgy csak tanú jelenlétében végezhető el az ellenőrzés. Az ellenőrzés során a belső adatvédelmi felelős betartva a fokozatosság elvét első lépésként az adott fájl, információ ellenőrzésére kerül sor. Amennyiben ennyiből megállapítható, hogy ez a munkáltatói tevékenység személyes adathoz való hozzáférést eredményezhet, úgy munkáltató nem tekinti meg, illetve nem nyitja meg az adott fájlt, leírást. Amennyiben nem valószínűsíthető a személyes adathoz való hozzáférés, úgy a belső adatvédelmi felelős jogosult az adott információ egység, adat megtekintésére, áttanulmányozására. Az ellenőrzés során, ha a belső adatvédelmi felelős talál nem a munkavégzéshez kapcsolódó személyes adatokat, magán tartalmakat, akkor annak törlésére felszólítja a munkavállalót, aki az adott tartalmak törlését köteles haladéktalanul elvégezni. Az eszközökön tárolt adatokról, információkról biztonsági másolat nem készül.

Az ügyvezető feladata tájékoztatni ellenőrzés előtt a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról, amelyek:

* az ellenőrzés célja: (pl. annak ellenőrzése, hogy sérül-e az adatbiztonság)
* eljárási szabályok, lépések: munkavállaló tájékoztatása ellenőrzésről, a technikai eszközbe való belépés, ellenőrző személy szemrevételezi a fájlokat, információ egységeket, egyeztetés munkavállalóval, hogy melyek a személyes adatokkal érintett fájlok, információs egységek, kötetlen formátumú ellenőrzési jegyzőkönyv megírása, aláírása)
* munkavállaló tájékoztatása a jogorvoslati jogokról.

##### Munkáltató által biztosított mobiltelefon, telefon használata

A **MORGEN-RED Kft.** vezetőségedöntése alapján minden munkavállaló **csak a munkavégzésével kapcsolatban használhatja a Társaság által biztosított mobiltelefont, telefont**, **tiltja az általa biztosított eszközökön a magánélethez kapcsolódó tevékenységek végzését, személyes adatok kezelését, tárolását.** A kapcsolódó adatkezelés jogalapja: munkáltató jogos érdeke, ezért a Társaság elvégezte az Érdekmérlegelési tesztet, melyet minden munkavállalóval megismertet, ugyanakkor a munkáltatói tiltás miatt itt **nem kerül sor személyes adatok kezelésére.**

A Társaság üzleti titkainak védelme, üzleti tevékenységének titokban tartása, illetve a munkavégzés ellenőrzése céljából az ügyvezető **ellenőrizheti** a munkavállalók a Társaság által **biztosított telefonon, mobiltelefonon** folytatott munkavállalói tevékenységeket, az eszköz memóriáját, az eszközre és a hozzá csatlakoztatott eszközre vonatkozó biztonsági előírások betartását. Az ő felelőssége, hogy felhívja a munkavállalók figyelmét, hogy amennyiben a tiltás ellenére magáncélra is használja a munkavállaló a biztosított telefonokat, úgy esetlegesen védett személyes adataihoz, vagy az abból származó következtetésekhez való hozzáférés kockázatának teszi ki magát.

Az ügyvezető feladata szúrópróbaszerűen dokumentáltan **ellenőrizni a munkahelyi telefon, mobiltelefon használatával kapcsolatos szabályok betartását**, biztosítva az érintett munkavállaló jelenlét, amennyiben ez mégsem lehetséges (pl. betegség, baleset, szabadság), úgy csak tanú jelenlétében végezhető el az ellenőrzés. Az ellenőrzés során a belső adatvédelmi felelős betartva a fokozatosság elvét első lépésként az adott információ ellenőrzésére kerül sor. Amennyiben ennyiből megállapítható, hogy ez a munkáltatói tevékenység személyes adathoz való hozzáférést eredményezhet, úgy munkáltató nem tekinti meg, illetve nem nyitja meg az adott fájlt, információ egységet. Amennyiben nem valószínűsíthető a személyes adathoz való hozzáférés, úgy a belső adatvédelmi felelős jogosult az adott információ egység, fájl, adat megtekintésére, áttanulmányozására. Az ellenőrzés során, ha az ügyvezető talál nem a munkavégzéshez kapcsolódó személyes adatokat, magán tartalmakat, akkor annak törlésére felszólítja a munkavállalót, aki az adott tartalmak törlését köteles haladéktalanul elvégezni. Az eszközökön tárolt adatokról, információkról biztonsági másolat nem készül.

Az ügyvezető felelős feladata tájékoztatni ellenőrzés előtt a munkavállalókat az ellenőrzéssel kapcsolatos lényeges információkról, amelyek:

* az ellenőrzés célja: (pl. annak ellenőrzése, hogy sérül-e az adatbiztonság)
* eljárási szabályok, lépések: munkavállaló tájékoztatása ellenőrzésről, a telefon eszközbe való belépés, ellenőrző személy szemrevételezi a fájlokat, információ egységeket, egyeztetés munkavállalóval, hogy melyek a személyes adatokkal érintett fájlok, információs egységek, kötetlen ellenőrzési jegyzőkönyv megírása, aláírása)
* munkavállaló tájékoztatása a jogorvoslati jogokról.

### Jogi kötelezettség teljesítése érdekében történő adatkezelés

A Társaságnál a **jogi kötelezettség teljesítése** jogalapon alapuló adatkezelés az érintett hozzájárulásától független, mivel az adatkezelést jogszabály határozhatta meg.

A belső adatvédelmi felelős felelőssége, hogy az adatkezelés kötelező jellegétől függetlenül az érintett magánszeméllyel az adatkezelés megkezdése előtt közölje, hogy az adatkezelés kötelező és nem kerülhető el, valamint a 9.2.1 fejezet szerint **megfelelő tájékoztatást adjon számára az adatai kezelésével kapcsolatos minden jelentős tényről**.

#### Adatkezelés adó- és társadalombiztosítási kötelezettségek teljesítése céljából

A **MORGEN-RED Kft.** a különböző adó- és társadalombiztosítási jogszabályokban előírt adó- és járulékkötelezettségek teljesítése (adó-, adóelőleg, járulékok megállapítása, bérszámfejtés, társadalombiztosítási ügyintézés) céljából, **jogi kötelezettség teljesítése jogalappal** kezeli azon érintett magánszemélyek (munkavállalók családtagjai, egyéb juttatásban részesülők, stb.) adótörvényekben előírt személyes adatait, **amely személyekkel kifizetői (Art. 7.§ 31.) jogviszonyban áll.**

**Adatkezelés célja**: adó- és társadalombiztosítási jogszabályokban előírt adó- és járulékkötelezettségek teljesítése kifizetői jogviszonyban álló magánszemélyek részére

**Az adatkezelés jogalapja:** jogi kötelezettség teljesítése

**Kezelt adatok lehetnek:** Art. 50.§ szerint a név, korábbi név, nem, állampolgárság, a természetes személy adóazonosító jele, társadalombiztosítási azonosító jel (TAJ szám), és a jogszabályban előírt további adatok, valamint amennyiben az adójogszabályok ehhez jogkövetkezményt fűznek, az adatkezelő kezelheti a munkavállalók egészségügyi (Szja. 40.§) és szakszervezeti (Szja. 47.§(2) b.) tagságra vonatkozó adatokat adó és járulékkötelezettségek teljesítés (bérszámfejtés, társadalombiztosítási ügyintézés) céljából

**Az adatok felelősei és címzettjei**: ügyvezető, irodavezető és az adatfeldolgozó: Eden&LLoyd Kft. (Halmai Gábor)

**Az adatok tárolásának időtartama**: a jogi kötelezettséget előíró jogszabályokban meghatározott időtartam

**Adattárolás helye, módja**: papír alapon a munkavállaló munkaügyi dossziéjában, illetve elektronikusan Iwise vállalatirányítási rendszerben.

A Társaság a 9.2.1 fejezet szerinti megfelelő **tájékoztatás ad** az érintett magánszemélyek számára az adatai kezelésével kapcsolatos minden jelentős tényről az adatkezelés megkezdése előtt.

#### Adatkezelés pénzmosás elleni kötelezettségek teljesítése céljából

A **MORGEN-RED Kft.** a **pénzmosás és a terrorizmus finanszírozása megelőzése és megakadályozása céljából, jogi kötelezettség teljesítése jogalappal** kezeli meghatározott ügyfelei, annak képviselője és tényleges tulajdonosai személyes adatait a Pmt. szerint.

**Adatkezelés célja**: pénzmosás és a terrorizmus finanszírozása megelőzése és megakadályozása

**Az adatkezelés jogalapja:** jogi kötelezettség teljesítése

**Kezelt adatok lehetnek:** természetes személy családi és utónevét, születési családi és utónevét, állampolgárságát, születési helyét, idejét, anyja születési nevét, lakcímét, ennek hiányában tartózkodási helyét, azonosító okmányának típusát és számát, lakcímet igazoló hatósági igazolványa számát, a bemutatott okiratok másolatát

**Az adatok felelősei és címzettjei**: ügyvezető

**Az adatkezelés időtartama**: jogszabályban meghatározott, azaz az ügyfél/üzleti kapcsolat megszűnésétől, illetve az ügyleti megbízás teljesítésétől számított 8 év a Pmt. 56.§(2) szerint

**Adattárolás helye és módja:** papír alapú adatkezelés során az irodai széfben

A Társaság a 9.2.1 fejezet szerinti megfelelő **tájékoztatás ad** az érintett magánszemélyek számára az adatai kezelésével kapcsolatos minden jelentős tényről az adatkezelés megkezdése előtt.

#### A Levéltári törvény szerint maradandó értékű iratokra vonatkozó adatkezelés

A **MORGEN-RED Kft.** **jogi kötelezettség teljesítése** jogalappal kezeli a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (Levéltári törvény) szerint **maradandó értékűnek minősülő iratait** abból a célból, hogy a Társaság irattári anyagának maradandó értékű része épségben és használható állapotban a jövő nemzedékei számára is fennmaradjon.

**Adatkezelés célja**: hogy a Társaság irattári anyagának maradandó értékű része jövő nemzedékei számára fennmaradjon

**Az adatkezelés jogalapja**: jogi kötelezettség teljesítése

**Kezelt adatok lehetnek**: jogszabály szerint maradandó értékűnek minősülő iratokban kezelt személyes adatok

**Az adatok felelősei és címzettjei**: ügyvezető

**Az adatkezelés időtartama**: közlevéltár részére történő átadásig

**Adattárolás helye és módja**: papír alapú adatkezelés során az irodai széfben

#### Fogyasztóvédelmi ügyintézés, reklamációk adatkezelése

A **MORGEN-RED Kft.** **jogi kötelezettség teljesítése** jogalappal kezeli a fogyasztóvédelemről szóló 1997. évi CLV. törvény, az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény értelmében a **reklamációk és a termékekkel, szolgáltatásokkal kapcsolatosan felmerülő minőségi kifogások kezelése céljából** vevők, ügyfelek személyes adatait.

**Adatkezelés célja**: reklamáció, termékekkel, szolgáltatásokkal kapcsolatosan felmerülő minőségi kifogások kezelése

**Az adatkezelés jogalapja:** jogi kötelezettség teljesítése

**Kezelt adatok lehetnek:** vevők, ügyfelek észrevételei, kifogásai, érintett a kötelezően megadandó adatokon (név és lakcím) kívül önkéntesen megadhat egyéb adatokat is (pl. elérhetőség, e-mailcím, telefonszám), fogyasztó által bemutatott iratok, dokumentumok és egyéb bizonyítékok tartalmazhatnak személyes adatot

**Az adatok felelősei és címzettjei**: vevőszolgálati vezető

**Az adatkezelés időtartama**: jogszabályban meghatározott 5 év

**Adattárolás helye és módja:** elektronikusan e-mailben

A Társaság a 9.2.1 fejezet szerinti megfelelő **tájékoztatás ad** az érintett magánszemélyek számára az adatai kezelésével kapcsolatos minden jelentős tényről az adatkezelés megkezdése előtt.

### Szerződéshez kapcsolódó adatkezelések

A **Rendelet** szerint lehetőség van személyes adatok kezelésére, ha az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett magánszemély az egyik fél, vagy az adatkezelés, adatfelvétel a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

#### Szerződő magánszemély ügyfelek, partnerek adatainak kezelése

A **MORGEN-RED Kft.** a **vevők és a szállítók nyilvántartása céljából, a szerződés teljesítése jogalappal** a szerződés megkötése, teljesítése, megszűnése céljából kezel személyes adatokat, figyelembe véve az **adattakarékosság elvét**. Ennek alapján a Társasággal vevőként, szállítóként szerződött természetes személyek adatai közül csak az esetenként külön-külön legszükségesebbek kerülnek adatkezelés alá.

**Adatkezelés célja**: megrendelés, vásárlás teljesítése, ügyfél kapcsolat megvalósítása

**Az adatkezelés jogalapja:** szerződés teljesítése

**Kezelt adatok lehetnek:** természetes személy családi és utónevét, postázási/értesítési címe, telefonszáma, e-mail címe, honlap-címét, bankszámlaszáma, online azonosítója (felhasználónév, jelszó)

**Az adatok felelősei és címzettjei**: vevőszolgálat vezetője, vevőszolgálati munkatársak, irodavezető

**Az adatkezelés időtartama**: jogszabályban meghatározott, 8 év a Sztv. szerint

**Adattárolás helye és módja:** elektronikusan Iwise vállalatirányítási rendszerben CRM moduljában

Az ezen a jogalapon alapuló adatkezelés jogszerűnek minősül akkor is, ha az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

A Társaság a 9.2.1 fejezet szerinti megfelelő **tájékoztatás ad** az érintett magánszemélyek számára az adatai kezelésével kapcsolatos minden jelentős tényről az adatkezelés megkezdése előtt.

#### Természetes személy képviselők, kapcsolattartók elérhetőségi adatainak kezelése

A Társaság az üzletfelek **természetes személy képviselőinek, kapcsolattartóinak nyilvántartása céljából, a szerződés teljesítése jogalappal** üzleti kapcsolattartás, szerződés kötése céljából kezel személyes adatokat, figyelembe véve az **adattakarékosság elvét**. Ennek alapján az üzleti partnereket képviselő, kapcsolattartó természetes személyek adatai közül csak a legszükségesebbek kerülnek adatkezelés alá.

**Adatkezelés célja**: nem magánszemély ügyféllel kötött szerződés teljesítése, üzleti kapcsolattartás

**Az adatkezelés jogalapja:** szerződés teljesítése

**Kezelt adatok lehetnek:** természetes személy családi és utónevét, képviselt cég, intézménybeli beosztása, címe, telefonszáma, e-mail címe, online azonosítója

**Az adatok felelősei és címzettjei**: vevőszolgálat vezetője, vevőszolgálati munkatársak, irodavezető

**Az adatkezelés időtartama**: jogszabályban meghatározott, 8 év a Sztv. szerint

**Adattárolás helye és módja:** elektronikusan Iwise vállalatirányítási rendszerben CRM moduljában

A Társaság a 9.2.1 fejezet szerinti megfelelő **tájékoztatás ad** az érintett magánszemélyek számára az adatai kezelésével kapcsolatos minden jelentős tényről az adatkezelés megkezdése előtt.

### Érintett hozzájárulása alapján történő adatkezelés

A Társaságnál a **Rendelet** előírásait betartva, **hozzájáruláson alapuló adatkezelés esetén az érintett írásbeli hozzájárulását adja a személyes adatai kezeléséhez**.

A hozzájárulás formai kötöttség nélküli, de az **utólagos bizonyíthatóság** papír- vagy elektronikus alapú írásbeli hozzájárulást igényel. Határozott, önkéntes hozzájárulásnak minősül az is, ha az érintett az adatkezelő által fenntartott internetes honlapján kifejezett cselekménnyel bejelöl egy erre vonatkozó négyzetet, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó beállításokat hajt végre. A hallgatás, az előre bejelölt ellenőrző ablak elfogadtatása vagy a passzív eltűrés nem minősül hozzájárulásnak.

Egy hozzájárulás egy adatkezelési cél érdekében végzett adatkezeléshez való hozzájárulást jelenti, így, ha az adatkezelőnek **több adatkezelési célja van, akkor az érintett személy hozzájárulását külön-külön be kell szerezni**.

A **MORGEN-RED Kft.**, az adatkezelő vezetősége megfelelő intézkedéseket hozott annak érdekében, elősegítse a **Rendelet**ben szereplő összes **érintett személy jogai**nak – a visszavonás jogának is - **gyakorlását**, melynek részletes leírása jelen szabályzat 9. fejezetében található.

#### Weboldalon történő adatkezelés

**A MORGEN-RED Kft. a honlapján tájékoztatja látogatóit, hogy cookie-kat nem alkalmaz a weboldalán, így adatkezelésre nem kerül sor.**

A Sütik (cookie-k)  rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl.: egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Az Európai Bizottság irányelvei alapján cookie-kat -kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek- csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni.

Amennyiben a Társaság a későbbiekben a honlapján cookie-kat alkalmazna, akkor előtte a belső adatvédelmi felelős feladata a **szükséges felhasználói tájékoztatók elkészítése és a weboldalon történő megjelenítése**, ahol figyelembe kell vennie a következőket:

* A felhasználó hozzájárulását nem igénylő sütik esetében a honlap első látogatása során kell tájékoztatást nyújtani. Nem szükséges, hogy a cookie-ra vonatkozó tájékoztató teljes szövege megjelenjen a honlapon, elegendő, ha a honlap üzemeltetői röviden összefoglalják a tájékoztatás lényegét, és egy linken keresztül utalnak a teljes körű tájékoztató elérhetőségére.
* A hozzájárulást igénylő sütik esetében, a tájékoztatás kapcsolódhat a honlap első látogatásához is abban az esetben, ha a sütik alkalmazásával együtt járó adatkezelés már az oldal felkeresésével megkezdődik. Amennyiben a cookie alkalmazására a felhasználó által kifejezetten kért funkció igénybevételéhez kapcsolódik, akkor a tájékoztatás is megjelenhet e funkció igénybevételéhez kapcsolódóan. Ebben az esetben sem szükséges az, hogy a cookie-ra vonatkozó tájékoztató teljes szövege megjelenjen a honlapon, elegendő egy rövid összefoglaló a tájékoztatás lényegéről, és egy linken keresztül utalás a teljes körű tájékoztató elérhetőségére.

A Társaság így biztosítja, hogy a látogató a honlap információs társadalommal összefüggő szolgáltatásainak igénybevétele előtt és az igénybevétel során bármikor megismerhesse, hogy a Társaság mely adatkezelési célokból mely adatfajtákat kezel, ideértve az igénybe vevővel közvetlenül kapcsolatba nem hozható adatok kezelését is.

#### Regisztráció a Társaság honlapján

**A MORGEN-RED Kft. honlapján a regisztráló természetes személy az erre vonatkozó négyzet bejelölésével adhatja meg hozzájárulását személyes adatai hozzájáruláson alapuló kezeléséhez.** A hozzájárulás formai kötöttség nélküli, de az **utólagos bizonyíthatóság** elektronikus alapú írásbeli hozzájárulást igényel. Határozott, önkéntes hozzájárulásnak minősül, ha az érintett az adatkezelő által fenntartott internetes honlapján kifejezett cselekménnyel bejelöl egy erre vonatkozó négyzetet. Az előre bejelölt ellenőrző ablak elfogadtatása vagy a passzív eltűrés nem minősül hozzájárulásnak. Egy hozzájárulás egy adatkezelési cél érdekében végzett adatkezeléshez való hozzájárulást jelenti, így, ha az adatkezelőnek **több adatkezelési célja van, akkor az érintett személy hozzájárulását külön-külön be kell szerezni**.

A Társaság a 9.2.1 fejezet szerint megfelelő **tájékoztatás ad** a honlapon az érintett magánszemély számára az adatai kezelésével kapcsolatos minden jelentős tényről.

**Adatkezelés célja:** A honlapon nyújtott szolgáltatások teljesítése.

**Az adatkezelés jogalapja:** érintett hozzájárulása

**Kezelt adatok:** a hozzájárulással érintett adatkör; a természetes személy neve (vezetéknév, keresztnév), címe, telefonszáma, e-mail címe, online azonosító

**Az adatok felelősei és címzettjei**: vevőszolgálat vezetője, vevőszolgálati munkatársak, irodavezető

**Az adatkezelés időtartama**: regisztráció/szolgáltatás fennállásáig, a hozzájárulásban megjelölt időtartam vagy visszavonásig

**Adattárolás helye és módja:** elektronikusan Iwise vállalatirányítási rendszerben CRM moduljában

A Társaság, az adatkezelő vezetősége megfelelő intézkedéseket hozott annak érdekében, elősegítse a **Rendelet**ben szereplő összes **érintett személy jogai**nak – a visszavonás jogának is - **gyakorlását**, melynek részletes leírása jelen szabályzat 9. fejezetében található.

#### Adatkezelés WEB áruházában

A **MORGEN-RED Kft.** által **működtetett WEB áruházban történő vásárlás, szerződésnek minősül**, figyelembe véve a 2001. évi CVIII. törvényt, és a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól szóló 45/2014. (II. 26.) Kormány rendeletet. A Társaság a szolgáltató az információs társadalommal összefüggő szolgáltatás nyújtására irányuló szerződés létrehozása, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, az abból származó díjak számlázása, valamint az azzal kapcsolatos követelések érvényesítése céljából kezelheti a **WEB áruházban regisztráló, vásárló azonosításához** szükséges természetes **személyazonosító adatokat és lakcímet** a 2001. évi CVIII. törvény 13/A.§(1) bekezdés szerint **szerződés teljesítése** jogcímen, valamint a telefonszámát, e-mail címét, bankszámlaszámát, online azonosítóját az **érintett hozzájárulása alapján.**

A Társaság **számlázás céljából kezelheti** az információs társadalommal összefüggő szolgáltatás igénybevételével kapcsolatos természetes személyazonosító adatokat, lakcímet, valamint a szolgáltatás igénybevételének időpontjára, időtartamára és helyére vonatkozó adatokat, a 2001. évi CVIII. törvény 13/A.§(2) bekezdés szerint **szerződés teljesítése jogcímen**.

A Társaság a 9.2.1 fejezet szerint megfelelő **tájékoztatás ad** a honlapon az érintett magánszemély számára az adatai kezelésével kapcsolatos minden jelentős tényről.

**Adatkezelés célja:** szerződés létrehozása, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, az abból származó díjak számlázása, valamint az azzal kapcsolatos követelések érvényesítése

**Az adatkezelés jogalapja:** érintett hozzájárulása illetve szerződés teljesítése

**Kezelt adatok:** személyazonosító adatok, lakcím,telefonszám, e-mail cím, bankszámlaszám, online azonosító, szolgáltatás igénybevételének időpontjára, időtartamára és helyére vonatkozó adatok (fizetési, szállítási információk)

**Az adatok felelősei és címzettjei**: vevőszolgálat vezetője, vevőszolgálati munkatársak, irodavezető, adatfeldolgozók: Aréna Digital Kft. (IT tárhely szolgáltató), GLS (futárszolgálat munkavállalói a szállítási adatok (név, cím, telefonszám) vonatkozásában).

**Az adatkezelés időtartama**: a regisztráció/szolgáltatás fennállásáig, vagy az érintett hozzájárulása visszavonásáig, vásárlás esetén a vásárlás évét követő 5 évig.

**Adattárolás helye és módja:** elektronikusan Iwise vállalatirányítási rendszerben

A Társaság, az adatkezelő vezetősége megfelelő intézkedéseket hozott annak érdekében, elősegítse a **Rendelet**ben szereplő összes **érintett személy jogai**nak – a visszavonás jogának is - **gyakorlását**, melynek részletes leírása jelen szabályzat 9. fejezetében található.

## Adatfeldolgozás

A **MORGEN-RED Kft.** betartja a **Rendelet** 28. cikk rendelkezéseit, amely szerint, ha az **adatkezelést az adatkezelő nevében más végzi**, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek **megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.**

**Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe**. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

Az adatfeldolgozó által **végzett adatkezelést** az uniós jog vagy tagállami jog alapján létrejött olyan – **az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó** –**szerződésnek** vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben.

A szerződés vagy más jogi aktus különösen előírja, hogy az adatfeldolgozó:

* a **személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli** – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja,
* biztosítja azt, hogy a személyes adatok kezelésére feljogosított **személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak,**
* meghozza a Rendelet 32. cikkben előírt intézkedéseket,
* az adatkezelés jellegének figyelembevételével **megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt** abban, hogy teljesíteni tudja kötelezettségét a **Rendelet** III. fejezetben foglalt **érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása** tekintetében,
* segíti az adatkezelőt a **Rendelet** 32–36. cikk szerinti **kötelezettségek teljesítésében**, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
* az adatkezelési szolgáltatás nyújtásának **befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl, vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő**,
* az adatkezelő rendelkezésére **bocsát minden olyan információt, amely meghatározott kötelezettségek teljesítésének igazolásához szükséges**, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

A **MORGEN-RED Kft**., mint adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti ezt a rendeletet vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.

Ha az adatfeldolgozó bizonyos, az adatkezelő nevében végzett konkrét adatkezelési tevékenységekhez **további adatfeldolgozó szolgáltatásait is igénybe veszi**, uniós vagy tagállami jog alapján létrejött szerződés vagy más jogi aktus útján erre a **további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni**, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött szerződésben vagy egyéb jogi aktusban szerepelnek. Különösen úgy, hogy a **további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen e rendelet követelményeinek**. Ha a további adatfeldolgozó **nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért**.

### Adatfeldolgozói garancianyújtás

**A MORGEN-RED Kft. adatfeldolgozóként garantálja – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – hogy a Rendelet követelményeinek teljesülését biztosító technikai és szervezési intézkedéseket végrehajtja, ide értve az adatkezelés biztonságát is.**

A Társaság vállalja, hogy a megbízó adatkezelő rendelkezésére bocsát minden olyan információt, amely az adatfeldolgozó igénybevételére vonatkozó jogi rendelkezéseknek való megfelelés igazolásához szükséges.

A Társaság az adatfeldolgozó tevékenysége során **biztosítja, hogy az érintett személyes adatokhoz való hozzáférésre feljogosított személyek** – ha jogszabályon alapuló megfelelő titoktartási kötelezettség hatálya alatt egyébként nem állnak – **az általuk megismert személyes adatok vonatkozásában titoktartási kötelezettséget vállaljanak.**

A **MORGEN-RED Kft**., mint adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével **megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében**, hogy **a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.** Intézkedéseket hoz annak biztosítására, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek **kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat**, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket. Gondoskodik arról, hogy **a tárolt adatokhoz belső rendszeren keresztül vagy közvetlen hozzáférés útján kizárólag az arra feljogosított személyek, és kizárólag az adatkezelés céljával összefüggésben férjenek hozzá.** Gondoskodik a felhasznált eszközök szükséges, rendszeres karbantartásáról, fejlesztéséről. Az adatokat tároló eszközt megfelelő fizikai védelemmel ellátott zárt helyiségben helyezi el, gondoskodik annak fizikai védelméről is. Az adatfeldolgozói feladatok megfelelő ellátása érdekében **megfelelő ismerettel és gyakorlattal rendelkező személyeket vesz igénybe.**

## Adattovábbítás

A **MORGEN-RED Kft.** betartja a **Rendelet** minden rendelkezését az adattovábbításra vonatkozóan. Az adattovábbítással kapcsolatos információk a [**https://www.gdpreg.hu**](https://www.gdpreg.hu) **alkalmazás Adatkezelési tevékenységek nyilvántartása** menüpontja szerint kerülnek tárolásra**.**

**A Társaság jelenleg nem továbbít személyes adatokat harmadik országokba vagy nemzetközi szervezetek részére.**

Amennyiben erre a későbbiekben sor kerülne a Társaság vezetősége betartja a **Rendelet** V. Fejezet vonatkozó előírásait, és figyelembe veszi a **Rendelet** (101-116)-t.

A Társaság vezetősége felelős azért, amennyiben személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerülne sor, az **érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan** a **Rendelet** 46. cikk szerinti megfelelő garanciákról.

A **Rendelet** (101) szerint; A nemzetközi kereskedelem és a nemzetközi együttműködés bővítéséhez szükség van a személyes adatoknak az Unión kívüli országok és a nemzetközi szervezetek viszonylatában megvalósuló forgalmára. Az ilyen forgalom növekedése új kihívásokat és problémákat támaszt a személyes adatok védelme tekintetében. Mindazonáltal a személyes adatoknak az Unióból harmadik országbeli adatkezelőknek, adatfeldolgozóknak, egyéb címzetteknek vagy nemzetközi szervezetek részére történő továbbítása esetén nem sérülhet a természetes személyeknek az Unióban e rendelettel biztosított védelem szintje, és annak fenn kell maradnia az ilyen személyes adatoknak az adott harmadik országból vagy nemzetközi szervezettől ezt követően ugyanazon vagy másik harmadik országbeli adatkezelőnek, adatfeldolgozónak vagy nemzetközi szervezetnek történő újbóli továbbítása esetén is. A harmadik országokba és a nemzetközi szervezetekhez való továbbítás csak a **Rendelet** teljes betartása mellett hajtható végre. A továbbításra akkor kerülhet csak sor, ha az adatkezelő vagy az adatfeldolgozó – e rendelet egyéb rendelkezéseire is figyelemmel – teljesíti a harmadik országok vagy nemzetközi szervezeteknek történő adattovábbításra vonatkozó, e rendeletben meghatározott feltételeket.

# Adatbiztonság

## Az adatkezelés biztonsága

**A MORGEN-RED Kft. vezetője felelős** azért,hogy figyelembe véve a szervezet méretét, a folyamatok bonyolultságát és kölcsönhatását, valamint a személyzet kompetenciáját **a Társaság informatikai biztonsági követelményrendszerét és környezetét meghatározza**, jelen szabályzat **10. fejezet**ében dokumentálva. A Társaság a 10.3 fejezetben leírtak szerint nyomon követi és megfelelő részletességgel dokumentálja az elektronikus információs rendszer biztonsági eseményeit, amelyekkel kapcsolatos tevékenységeket az elektronikus információs rendszerek biztonságáért felelős ügyvezető koordinálja.

A **MORGEN-RED Kft.** vezetősége elkötelezett, hogy a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

* a személyes adatok álnevesítését és titkosítását,
* a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét,
* 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,
* az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A Társaság vezetője felelős azért, hogy a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

A Társaság vezetősége törekszik arra, hogy a **Rendelet** 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozását felhasználhatja annak bizonyítása részeként, hogy az e cikk (1) bekezdésében meghatározott követelményeket teljesíti.

**A Társaság vezetősége jelen Adatkezelési szabályzat jóváhagyásával és rendszerbe állításával biztosítja, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat,** kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

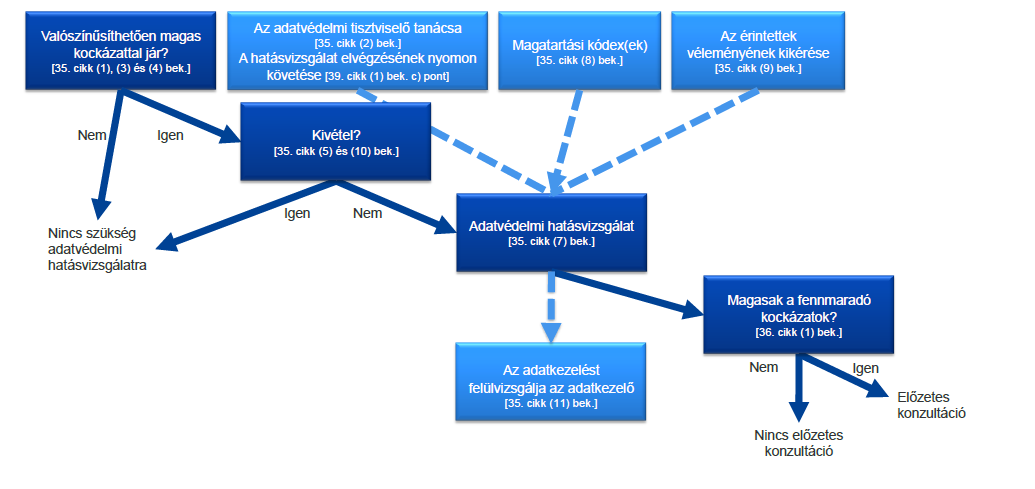
Az ügyvezető felelős azért, hogy

* A **titkosítással és az álnevesítéssel** kapcsolatos, lehetőségek, szakmai, technológiai eredményeket feltérképezze, a titkosítási és álnevesítési tevékenységek felelőseit kijelölje, és e tevékenységek végrehajtását jóváhagyja, irányítsa, ellenőrizze, és megfelelő szinten dokumentálja.
* A Társaság valamennyi adatkezelése tekintetében felmérje, majd meghatározza és megtegye azokat **a technikai és szervezési intézkedéseket** is a személyes adatok biztonsága érdekében, amelyek a jogi és számítástechnikai szempontokon túl is garantálják az érintettek jogait.
* Belső szabályozással, intézkedésekkel megakadályozza a személyes adatok véletlen vagy jogellenes sérülését, megváltoztatását, megsemmisítését, elvesztését, jogosulatlan nyilvánosságra hozatalát vagy az azokhoz való jogosulatlan hozzáférést.
* Az informatikai rendszert időszakosan **frissülő tűzfallal és vírusvédelemmel** védje.
* A Társaság biztosítsa az adatok és az azokat hordozó eszközök, iratok megfelelő fizikai és adminisztratív védelmét, az éppen munkavégzéssel érintett adatokhoz, fájlokhoz, iratokhoz csak a feladattal érintett jogosultak férhessenek hozzá, a személyzeti, a bér- és munkaügyi ás egyéb személyes adatokat tartalmazó papír alapú iratok biztonságosan el legyenek zárva.
* A Társaság a munkaügyi adatvédelmi szabályai szerint a személyes adatok védelme érdekében jogos érdeke jogalappal ellenőrizze az **elektronikus úton folytatott bejövő és kimenő információ áramlását.**

## Hatásvizsgálat módszertana

A **MORGEN-RED Kft**., mint adatkezelő felelőssége, hogy **Rendelet** előírásai szerint adatvédelmi hatásvizsgálatot végezzen. Az adatvédelmi hatásvizsgálat végzésére vonatkozó kötelezettség jól illeszkedik a **Rendeletben** hangsúlyosan megjelenő beépített és alapértelmezett adatvédelem elveihez, hiszen a szolgáltatásokat úgy kell megtervezni, hogy az adatvédelem már az első lépésektől kezdődően szempontként merüljön fel és az esetleges kockázatok felmérése és a szükséges kockázatkezelő intézkedések megtervezése, és végrehajtása megfelelően megtörténjen.

Az alábbi ábra a **Rendeletben** az adatvédelmi hatásvizsgálattal kapcsolatosan megfogalmazott elveket szemlélteti:



A hatásvizsgálat szorosan kapcsolódik a Rendeletnek megfelelő adatkezelési gyakorlat kialakítását és a megfelelés igazolását elváró ún. elszámoltathatóság alapelvéhez.

A **Rendelet** 35. cikk szerint, "ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, ***valószínűsíthetően magas kockázattal jár*** a természetes személyek jogaira és szabadságaira nézve, akkor ***az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez*** arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. [...]"

Az adatvédelmi hatásvizsgálat tehát egy olyan eljárás, amelynek során az adatkezelő, a Társaság a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja.

### Kockázatkezelés

A **MORGEN-RED Kft.** **vezetősége** az adatvédelmi hatásvizsgálat elvégzésére vonatkozó kötelezettségét a személyes adatok kezeléséből eredő kockáztok megfelelő kezelésére vonatkozó általános kötelezettséggel összefüggésben értelmezi.

A belső adatvédelmi felelős a **29-es Munkacsoport** iránymutatása szerint jár el, amely szerint:

„A **Rendelet**ben kifejezésre juttatott kockázatalapú megközelítéssel összhangban nem mindegyik adatkezelési művelet esetében kötelező adatvédelmi hatásvizsgálatot végezni. Ehelyett csak akkor van szükség adatvédelmi hatásvizsgálatra, ha az adatkezelés valamely fajtája „valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve” (a 35. cikk (1) bekezdése). **Azonban önmagában az a tény, hogy az adatvédelmi hatásvizsgálat elvégzésének kötelezettségét keletkeztető feltételek nem teljesülnek, semmit nem von le az adatkezelők azon általános kötelezettségéből, hogy intézkedéseket hajtsanak végre az érintettek jogait és szabadságait érintő kockázatok megfelelő kezelése érdekében.** **A gyakorlatban ez azt jelenti, hogy az adatkezelőknek folyamatosan értékelniük kell az adatkezelési tevékenységeikből eredő kockázatokat, hogy felismerjék, ha az adatkezelés valamely fajtája ’valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve’.”**

A „kockázat” olyan eshetőség, amely a súlyosság és valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit. Az adatbiztonsági kockázat értékelése során a személyes adatok kezelése jelentette olyan kockázatokat, mint például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés, mérlegelni kell, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.

A lehetséges kockázatok három csoportra oszthatók:

* 1. **Személyeket érintő kockázatok:**

• az adatok nem megfelelő nyilvánosságra hozatala növeli annak esélyét, hogy olyan adatokat is megosztanak, amelyeket jogszerűen nem lehetne,

• az adatkezelés célja megváltozhat, így az idő múlásával a tárolt adatokat másra használják fel az érintett tudta nélkül,

• adatbázisok összefésülése, amelynek köszönhetően olyan felhasználói profilok hozhatók létre, amelyekből új információk nyerhetők ki,

• azonosítók összekapcsolása, amely meggátolja az anonim felhasználást.

* 1. **Szervezeteket érintő kockázatok:**

• adatvédelmi hatóság álláspontjába vagy olyan jogszabályi előírásba való ütközés, melynek következményeként bírság vagy más szankciók is kiszabhatók,

• olyan problémák felmerülése, amelyekre csupán az adatkezelés elindítását követően derül fény, és a kijavításuk rendkívül költségigényes,

• az adatminimalizálás elvébe ütköző felesleges, készletező, esetleg többszöri adatgyűjtés, amely így csökkentheti az adatkezelés hatékonyságát,

• a bizonytalan és nem megfelelő adatkezelés a társadalomban bizalomvesztést eredményezhet, amely bevételcsökkenés formájában jelenhet meg.

• adatvesztés, amely az érintettek számára kárt okoz, valamint az érintettek részéről kártérítési igényt generál.

* 1. **Compliance-kockázatok:**

• az adatkezelés nem felel meg a tagállami hatóság állásfoglalásaiban foglaltaknak;

• az ágazat-specifikus előírásoknak; vagy

• az alkotmányjogi előírásoknak.

### Adatvédelmi hatásvizsgálat

A **MORGEN-RED Kft.** vezetősége elkötelezett az iránt, hogy a **Rendelet**ben meghatározott körülmények esetén a belső adatvédelmi felelős dokumentáltan adatvédelmi hatásvizsgálatot végezzen.

Ezek a következők:

* természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely **automatizált adatkezelésen** – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében **joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek**,
* **a személyes adatok különleges kategóriái** (9. cikk), **vagy a büntetőjogi felelősség** megállapítására vonatkozó határozatokra **és bűncselekményekre vonatkozó személyes adatok** (10. cikk) **nagy számban történő kezelése,**
* **nyilvános helyek nagymértékű, módszeres megfigyelése**.

Ezen túlmenően is **hatásvizsgálatot kell végezni** minden olyan adatkezelés tekintetében, amelyek **valószínűsíthetően magas kockázattal járnak az érintettekre nézve**.

Annak eldöntése során tehát, hogy szükséges-e adatvédelmi hatásvizsgálatot végezni elsődlegesen azt kell vizsgálnia a Társaság belső adatvédelmi felelősének, hogy mit jelent a **Rendelet** vonatkozásában a "kockázat", illetve a "magas kockázat" fogalma. A Társaság belső adatvédelmi felelősének segítséget nyújt, hogy a felügyeleti hatóságoknak (NAIH) össze kell állítania és nyilvánosságra kell hoznia azon adatkezelések listáját, amelyek tekintetében adatvédelmi hatásvizsgálatot kell végezni. Ezen túlmenően a felügyeleti hatóságok összeállíthatnak és közzétehetnek olyan listát is, amely azon adatkezeléseket tartalmazza, amelyek esetében nincs szükség hatásvizsgálat elvégzésére.

A belső adatvédelmi felelős a hatásvizsgálatok lefolytatásánál figyelembe veszi, hogy a kockázati tényezők azonosításában nagy szerepe lehet az érintettekkel való konzultációnak, valamint, hogy a **Rendelet** több veszélyforrást is kifejezetten megtilt, például a készletező adatkezelést vagy a hozzájárulás nélküli adattovábbítást.

A **Rendelet** szerint a hatásvizsgálat kiterjed legalább:

* a**tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére** (beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket);
* az adatkezelés céljaira figyelemmel **az adatkezelési műveletek szükségességi és arányossági vizsgálatára**;
* az érintett jogait és szabadságait érintő **kockázatok vizsgálatára**; és
* **a kockázatok kezelését célzó intézkedések bemutatására.**

**Minden szükséges hatásvizsgálatot dokumentáltan kell elvégeznie a belső adatvédelmi felelősének, vagy az általa megbízott munkatársnak a** [**https://www.gdpreg.hu**](https://www.gdpreg.hu) **alkalmazás Hatásvizsgálat menüpontja szerint.**

Bizonyos esetekben a Társaság, mint adatkezelő **mentesül** a hatásvizsgálat elvégzésének kötelezettsége alól, melyek:

* az adatkezelés valószínűsíthetően **nem jár magas kockázattal**,
* **egymáshoz hasonló típusú adatkezelési műveletek** esetében, amelyek egymáshoz hasonló magas kockázatokat jelentenek, **egyetlen hatásvizsgálat is elegendő**, azaz nem kell feltétlenül külön hatásvizsgálatot készíteni,
* a felügyeleti hatóság **azon listáján szerepel, amely szerint az adott kezelés tekintetében nem kötelező hatásvizsgálatot végezni, illetve a Rendeletben kizárásra kerül.**

A belső adatvédelmi felelős feladata, hogy szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén dokumentáltan értékelje azt, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

A belső adatvédelmi felelős felelőssége, hogy amennyiben az adatkezelés a Társaság (adatkezelő) által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően, a **Rendelet** szerint **konzultáljon a felügyeleti hatósággal** (NAIH), és a továbbiakban a NAIH iránymutatása szerint járjon el.

## Adatvédelmi incidensek

A Társaságnak, mint adatkezelőnek a felelőssége, hogy amint tudomására jut e**gy adatvédelmi incidens** (pl. felmerül a gyanú, hogy Társaság számítógépes biztonsági incidens áldozatává vált, vagy éppen ennek folyamata alatt van, a Társaság IT rendszere) azt **indokolatlan késedelem nélkül** (ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott) **bejelenteni köteles az illetékes felügyeleti hatóságnál (NAIH)**. Kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően **nem jár kockázattal a természetes személyek jogaira és szabadságaira** nézve. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

A belső adatvédelmi felelős feladata az érintettet indokolatlan késedelem nélkül **tájékoztatni** abban az esetben, ha az adatvédelmi incidens **valószínűsíthetően (**dokumentáltan**) magas kockázattal jár** a természetes személyek jogaira és szabadságaira nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket. **A tájékoztatásnak tartalmaznia kell annak leírását, hogy milyen jellegű az adatvédelmi incidens, valamint az érintett a természetes személynek szóló, a lehetséges hátrányos hatások enyhítését célzó javaslatokat.** **Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal (NAIH)**.

**A belső adatvédelmi felelős felelőssége megbizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében**. Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani. A felügyeleti hatóságnak történt bejelentés a **Nemzeti Adatvédelmi és Információszabadság Hatóság**nak a **Rendelet**ben meghatározott feladataival és hatásköreivel összhangban történő beavatkozását eredményezheti.

### Az adatvédelmi incidens kezelése

**A MORGEN-RED Kft. ügyvezetője elrendelte,** és erről minden belső és külső munkatárs tájékoztatást kapott, **hogy minden vélt vagy valós adatvédelmi incidensről késedelem nélkül, telefonon és e-mail-ben értesíti kell, a belső adatvédelmi felelőst. Az adatvédelmi incidenst észlelő személy köteles a tapasztalt jelenséget** **regisztrálni** (ha értelmezhető) **és haladéktalanul a belső adatvédelmi felelős rendelkezésére bocsátani** (pl. feljegyzés, képernyőkép, fotó, hibaüzenet, stb.).

Az adatvédelmi incidens bejelentésére vonatkozó kötelezettség vonatkozik a Társaság valamennyi alkalmazottjára, és közreműködő munkatársára, valamint a Társasággal szerződéses, vagy más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra a velük kötött megállapodás, vagy titoktartási nyilatkozatok alapján.

**Belső adatvédelmi felelős elérhetőségei:**

**Telefonszám: Domiter Zoltánné**

**E-mail cím: domiter.rita@morgenred.hu**

**A Társaság ügyvezetője miután értesült az adatvédelmi incidensről haladéktalanul megkezdi az incidens körülményeinek kivizsgálását és végrehajtsa a következőket,** mely szerint:

* a körülmények ismeretében **felméri a kockázatokat és meghatározza a kategóriát (**nincs/van/magas kockázat),
* szükség esetén eseti **szakértői csoportot hoz létre** az incidens körülményeinek kivizsgálására, akik segítik a munkáját,
* **értesíti a Társaság vezetőjét**,
* **meghatározza az értesítendők körét,**
* szükség szerint a **Nyilatkozat adatvédelmi incidens bekövetkezéséről** dokumentumot **közzéteszi** a Társaság honlapján,
* amennyiben az adatbiztonsági incidens **IT biztonsági esemény is egyben intézkedést tesz** észlelése után **annak megszüntetésére**, vagy az esemény jellegéből adódóan annak izolálására (az izolálást azonnal meg kell kezdeni, az érintett felek bevonásával), majd továbbiakban a **10.4.3 fejezetben** leírtak szerint jár el,
* **meghatározza az adatvédelmi incidens jellegét**, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
* **felméri az adatvédelmi incidensből eredő, valószínűsíthető következményeket**,
* **meghatározza az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket**, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket,
* az adatvédelmi incidensről, valamint annak életútjáról **jegyzőkönyvet készít**,
* **rögzíti az adatvédelmi incidenseket, az** <https://www.gdpreg.hu> alkalmazás **Adatvédelmi incidensek nyilvántartása** menüpontban, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket,
* indokolatlan késedelem nélkül, a 8.3.2 fejezet szerint bejelenti illetékes **Nemzeti Adatvédelmi és Információszabadság Hatóság**nak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve,
* amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár természetes személyek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül a 7.1.3.2 fejezet szerint **tájékoztatja az érintetteket** az adatvédelmi incidensről,
* amennyiben nem volt lehetséges az adatvédelmi incidenssel kapcsolatos információkat egyidejűleg közölni illetékes hatósággal, akkor azokat további indokolatlan késedelem nélkül később részletekben közli az **Nemzeti Adatvédelmi és Információszabadság Hatóság**gal,
* **irányítja a károk helyreállítását és a jogszerű működés visszaállítását,**
* **lezárja az adatvédelmi incidens kezelésének folyamatát és a kapcsolódó dokumentumokat.**

A **MORGEN-RED Kft.** ügyvezetője a belső adatvédelmi felelősselaz <https://www.gdpreg.hu> alkalmazás Adatvédelmi incidensek nyilvántartása menüpontban rögzített az adatvédelmi incidenshez kapcsolódó, és az incidensről felvett jegyzőkönyvben szereplő információkat az adatvédelmi incidens kezelésének lezárása után egy hónapon belül áttekinti. Ellenőrzi a **Rendelet**nek, valamint a Társaság személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, valamint áttekinti az érintettek jogainak védelmét szolgáló korrekciós intézkedéseket biztosító mechanizmusokat, és az incidensek kezelésére vonatkozó intézkedéseket, és azok eredményességét. Az ellenőrzés tapasztalatai szükség szerint beépülhetnek az adatvédelmi szabályozásba, illetve részét képezhetik a munkatársak képzésének, tovább képzésének.

### Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak

Az adatvédelmi incidenst a Társaság belső adatvédelmi felelőse indokolatlan **késedelem nélkül**, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes **Nemzeti Adatvédelmi és Információszabadság Hatóság**nak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Az adatvédelmi incidensről szóló bejelentést a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) mindenkori kapcsolati pontjára (<http://naih.hu/uegyfelszolgalat,--kapcsolat.html>) kell eljuttatni. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Az adatvédelmi incidens bejelentésekor meg kell adni a következőket:

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

Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

A Társaság belső adatvédelmi felelőse nyilvántartja az adatvédelmi incidenseket, az <https://www.gdpreg.hu> alkalmazás Adatvédelmi incidensek nyilvántartása menüpontban, így e nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze a **Rendelet** 33. cikk követelményeinek való megfelelést.

### Az érintett tájékoztatása az adatvédelmi incidensről

**A MORGEN-RED Kft. belső adatvédelmi felelőse felelős azért, hogy amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár természetes személyek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül tájékoztatja az érintetteket az adatvédelmi incidensről.**

Az **érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét** (beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát), és közölni kell az adatvédelmi incidens bejelentésekor közölt információkat. Azaz az érintettel közölni kell az . vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit, ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket, és a Társaság, az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

**A belső adatvédelmi felelősnek az adatkezelési incidensben érintettet nem kell tájékoztatnia, ha a következő feltételek bármelyike teljesül** (Rendelet, 34.cikk (3) szerint):

* az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat,
* az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg,
* a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Ha a Társaság, mint adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a Rendelet, 34.cikk (3) bekezdésben említett feltételek valamelyikének teljesülését, és ekkor nem kell az érintettet továbbra sem tájékoztatni.

# Az érintett jogai

**A Társaság,** az adatkezelő **vezetősége megfelelő intézkedéseket hozott annak érdekében, hogy az érintett magánszemélyek jogaira vonatkozóan a Rendelet III. fejezet** 12-23. cikk(figyelem véve az 5. szakaszban foglaltakat) **minden rendelkezését betartsa, és elősegíti a Rendeletben szereplő összes érintetti jog gyakorlását.**

**Az érintett magánszemélyek jogai a Rendelet szerint, röviden összefoglalva, a következők:**

* **Előzetes tájékoztatáshoz való jog**

Az érintett magánszemély bármikor jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról érthető, tömör tájékoztatást kapjon, ez a joga az adatkezelés megkezdését megelőzően is fennáll.

* **Hozzáférési jog**

Az érintett magánszemély jogosult arra, hogy az adatkezelőtől tömör, közérthető választ kapjon arra nézve, hogy személyes adatainak kezelését végzik-e aktuálisan, és ha igen, akkor jogosult arra, hogy a személyes adatokhoz és az uniós rendeletben meghatározott kapcsolódó információkhoz hozzáférést kapjon.

* **Helyesbítéshez való jog**

Az érintett magánszemély jogosult arra, hogy kérésére az adatkezelő - indokolatlan késedelem nélkül - helyesbítse a rá vonatkozó pontatlan személyes adatokat. Az érintett jogosult arra, hogy kérje a téves, hibás, hiányos személyes adatok módosítását, kiegészítését.

* **A törléshez/ ”elfeledtetéshez” való jog**

Az érintett magánszemély jogosult arra, hogy kérésére az adatkezelő - indokolatlan késedelem nélkül - törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha annak nincs jogi akadálya. Az érintettnek ez a joga különösen a hozzájárulása alapján kezelt személyes adataihoz kapcsolódóan áll fent, más jogalapok fennállta, így többek között a jogi kötelezettség teljesítése alapján kezelt adatok esetén pedig kifejezetten korlátozott ez a joga, illetve nem áll fent.

* **Az adatkezelés korlátozásához való jog**

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha bizonyos meghatározott feltételek teljesülnek. Ez az esetkör leginkább egy bizonyos adatkezelési állapot rögzítésére szolgál, amely akár egy jogvitás helyzet előzménye vagy már maga a konkrét vitás helyzet is lehet.

* **A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség**

Az adatkezelő minden olyan címzettet tájékoztat minden helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akikkel a személyes adatot közölték. Kivétel: nem várható el ezen kötelezettség teljesítése, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne.

* **Az adathordozhatósághoz való jog**

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

* **A tiltakozáshoz való jog**

Az érintett magánszemély jogosult arra, hogy bármikor tiltakozzon személyes adatainak kezelése ellen, ha az

* adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, illetve ha
* az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.
* **Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást**

Az érintett magánszemély jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – profilalkotás is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené. Az érintett magánszemély ilyenkor kérheti a kézi, emberi beavatkozást és döntésalkotást.

* **Kép- és hangrögzítésre alkalmas kamerával megfigyelt terület**

Az érintett magánszemély jogosult arra, hogy tájékoztatást kapjon a vagyonvédelmi kamerák működtetésével kapcsolatos adatkezelési szabályokról, a kamerák jellemzőiről és a kapcsolódó adatbiztonsági, használati és érintetti jogi kérdésekről. (7.1.3.7 fejezet)

* **Az érintett tájékoztatása az adatvédelmi incidensről**

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, abban az esetben az adatkezelő - indokolatlan késedelem nélkül - tájékoztatja az érintettet az adatvédelmi incidensről.

* **A felügyeleti hatóságnál történő panasztételhez való jog (hatósághoz való fordulás joga)**

Az érintett magánszemély jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti az uniós adatvédelmi rendeletet.

* **A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog**

Minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben. Ez a jog akkor is fennáll, ha a felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

* **Az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog**

Minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak az uniós rendeletnek nem megfelelő kezelése következtében megsértették a jogait. Az bírósági illetékességi szabályok szerinti Törvényszék jogosult az eljárásra.

Az érintett magánszemélyek jogait a **Rendelet** III szakasz 12-23. cikk- szerint részletesen, a következő 9.1 - 9.6 fejezetek tartalmazzák.

A belső adatvédelmi felelős felelős azért, hogy a Társasághoz az adatkezelőhöz érkezett érintetti kérelem beérkezésétől számított 30 napon a **Rendelet** alapján eljárjon jelen szabályzat 9.7 fejezetében leírtak szerint.

## Átláthatóság és intézkedések

A Társaság, az adatkezelő megfelelő intézkedéseket hozott annak érdekében, hogy **az érintett részére a Rendelet** 13. és a 14. cikkben említett valamennyi információt és a 15–22. és 34. cikk szerinti, **minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa**. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

A Társaság elősegíti az érintettek **Rendelet** 15–22. cikk szerinti jogainak gyakorlását, és **általában díjmentesen, késedelem nélkül**, de mindenféleképpen a kérelem beérkezésétől számított **egy hónapon belül tájékoztatja** az érintettet a **Rendelet** 15–22. cikk szerinti kérelem nyomán hozott intézkedésekről, illetve szükség esetén, 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. Amennyiben a Társaságnak megalapozott kétségei vannak a **Rendelet** 15–21. cikk szerinti kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.

## Tájékoztatás és a személyes adatokhoz való hozzáférés

### Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik

Amennyiben a Társaság személyes adatokat gyűjt, a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

* a **Társaság és képviselőjének a kiléte és elérhetőségei**,
* az . elérhetőségei, ha van ilyen,
* a **személyes adatok tervezett kezelésének célja**, valamint **az adatkezelés jogalapja**,
* a Társaság (adatkezelő) vagy harmadik fél jogos érdekei **Rendelet** 6. cikk (1) bekezdésének f) pontján alapuló adatkezelés esetén,
* adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen,
* harmadik országba vagy nemzetközi szervezet részére továbbítani kívánt személyes adatok esetén megfelelő és alkalmas garanciák megjelölése, illetve elérhetőségére való hivatkozás megadása.

A Társaság a személyes adatok megszerzésének időpontjában, annak érdekében, hogy a tisztességes és átlátható adatkezelést biztosítsa, az érintettet a következő kiegészítő információkról tájékoztatja:

* a **személyes adatok tárolásának időtartamáról**, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól,
* az **érintett** azon **jogáró**l, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról,
* a **Rendelet** 6. cikk (1) bekezdésének a) pontján vagy a 9. cikk (2) bekezdésének a) pontján alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő **visszavonásához való jog**, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
* a felügyeleti hatósághoz címzett **panasz benyújtásának jogáról**,
* arról, hogy a **személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul** vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása.
* a **Rendelet** 22. cikk (1) és (4) bekezdésében említett **automatizált döntéshozatalról,** ideértve a **profilalkotás**t is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

**A belső adatvédelmi felelős felelőssége, hogy amennyiben a Társaság személyes adatokat gyűjt, a személyes adatok megszerzésének időpontjában dokumentáltan az érintett rendelkezésére bocsátja jelen fejezetben előírt információk mindegyikét egy a** [**https://www.gdpreg.hu**](https://www.gdpreg.hu) **alkalmazásban generált vonatkozó adatkezelési tájékoztatón.**

Amennyiben a Társaság a személyes adatokon a gyűjtésük **céljától eltérő célból további adatkezelést** kíván végezni, a **további adatkezelést megelőzően tájékoztatja** az érintetteket erről az eltérő célról és minden szükséges releváns kiegészítő információról.

**Nem kell információkat adni** személyes adatok gyűjtésekor, ha és amilyen mértékben **az érintett már rendelkezik az információkkal**.

### Az előzetes tájékoztatás Infotv. 20. § (2) bekezdése szerinti követelményei

Az érintettek a megfelelő előzetes tájékoztatásához az Infotv. előírásait és a NAIH vonatkozó ajánlásait is figyelembe veszi a Társaság, ahol az előzetes tájékoztatásra vonatkozó követelmények:

* közérthető, olvasható, áttekinthető, igazodik az érintettek köréhez, rendelkezésre áll, elérhető, nem jognyilatkozat,
* ismerteti az adatkezelő egyedi adatkezelését,
* megnevezi az adatkezelőt (név, cím, (cégjegyzékszám), postai cím, elektronikus elérhetőség (folyamatosan figyelt elérhetőség), honlap címe, telefonszám (egyértelműen azonosítható)
* megadja az adatkezelés célját (közérthető, egyértelmű, valós indok, kapcsolódó adatok köréről való tájékoztatás, szükséges mérték megadása, pontosság (kamerarendszerek)),
* ismerteti az adatkezelés jogalapját,
* meghatározza a kezelt adatok körét (táblázat, szükséges mérték), az adatkezelés időtartamát, tájékoztat adatfeldolgozó igénybevételéről,
* megadja az adatok megismerésére jogosult személyek körét
* az adatbiztonsági intézkedésekről és az Infotv. 6. § (5) bekezdésén alapuló adatkezelésről szóló tájékoztatást,
* valamint az érintettek jogait és jogérvényesítési lehetőségeit.

### Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg

Amennyiben a **MORGEN-RED Kft**. az adatkezelő a személyes adatokat nem az érintettől szerezte meg, az érintett rendelkezésére bocsátja a következő **információkat**:

* a **Társaság és képviselőjének a kiléte és elérhetőségei**,
* az . elérhetőségei, ha van ilyen,
* a **személyes adatok tervezett kezelésének célja**, valamint **az adatkezelés jogalapja**,
* az érintett személyes adatok kategóriái,
* a **személyes adatok címzettjei**, illetve a címzettek kategóriái, ha van ilyen,
* adott esetben annak ténye, hogy az adatkezelő valamely harmadik országbeli címzett vagy valamely nemzetközi szervezet részére kívánja továbbítani a személyes adatokat. Továbbá a **Bizottság** megfelelőségi határozatának léte vagy annak hiánya, vagy a **Rendelet**  46. cikkben, a 47. cikkben vagy a 49. cikk (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az ezek másolatának megszerzésére szolgáló módokra, vagy az elérhetőségükre való hivatkozás.

A Társaság, az adatkezelő az érintett rendelkezésére bocsátja az érintettre nézve tisztességes és átlátható adatkezelés biztosításához szükséges következő **kiegészítő információkat**:

* a személyes adatok **tárolásának időtartama**, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
* ha az adatkezelés a **Rendelet** 6. cikk (1) bekezdésének f) pontján alapul, az **adatkezelő vagy harmadik fél jogos érdekeiről**,
* az érintett azon joga, hogy **kérelmezheti** az adatkezelőtől a rá vonatkozó személyes adatokhoz való **hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat** a személyes adatok kezelése ellen, valamint az érintett **adathordozhatósághoz** való joga,
* a **Rendelet** 6. cikk (1) bekezdésének a) pontján vagy a 9. cikk (2) bekezdésének a) pontján alapuló adatkezelés esetén a **hozzájárulás bármely időpontban való visszavonásához való jog**, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
* a valamely felügyeleti hatósághoz címzett **panasz benyújtásának joga**,
* a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e; és
* a **Rendelet** 22. cikk (1) és (4) bekezdésében említett **automatizált döntéshozatal ténye**, ideértve a **profilalkotást** is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

A Társaság, az adatkezelő jelen fejezetben meghatározott tájékoztatást az alábbiak szerint adja meg:

* a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül;
* ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy
* ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

Ha az adatkezelő a személyes adatokon a megszerzésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően **tájékoztatnia kell az érintettet** erről az eltérő célról **és minden** **releváns kiegészítő információról**.

**A belső adatvédelmi felelős felelőssége, hogy amennyiben a Társaság személyes adatokat nem az érintettől szerezte meg, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül dokumentáltan az érintett rendelkezésére bocsátja jelen fejezetben előírt információk mindegyikét egy a** [**https://www.gdpreg.hu**](https://www.gdpreg.hu) **alkalmazásban generált vonatkozó adatkezelési tájékoztató formájában.**

**Nem kell tájékoztatást, információkat adni**, ha a Társaság, az adatkezelő a személyes adatokat nem az érintettől szerezte meg, ha és amilyen mértékben

* az érintett **már rendelkezik az információkkal**,
* a szóban forgó információk rendelkezésre bocsátása **lehetetlennek** bizonyul, vagy **aránytalanul nagy erőfeszítést igényelne**, különösen a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, a **Rendelet** 89. cikk (1) bekezdésében foglalt feltételek és garanciák figyelembevételével végzett adatkezelés esetében, vagy amennyiben a **Rendelet** 14. cikk (1) bekezdésében említett kötelezettség valószínűsíthetően lehetetlenné tenné, vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. Ilyen esetekben az adatkezelőnek megfelelő intézkedéseket kell hoznia – az információk nyilvánosan elérhetővé tételét is ideértve – az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében,
* az **adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog**, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik,
* a személyes adatoknak valamely **uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség** alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia.

### Az érintett hozzáférési joga

Az érintett jogosult arra, hogy a Társaságtól, az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

* az **adatkezelés céljai**,
* az érintett személyes **adatok kategóriái**,
* azon **címzettek vagy címzettek kategóriái**, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket,
* adott esetben a személyes **adatok tárolásának tervezett időtartama**, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
* az érintett azon joga, hogy **kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen**,
* a valamely felügyeleti hatósághoz címzett **panasz benyújtásának joga**,
* ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ,
* a 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a **Rendelet** 46. cikk szerinti megfelelő garanciákról.

**A Társaság,** az adatkezelő **az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja jelen szabályzat 9.7 fejezete szerint.**

Az érintett által kért további másolatokért a Társaság az adminisztratív költségeken alapuló, észszerű mértékű díjat számít fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

## Helyesbítés és törlés

### A helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére a **MORGEN-RED Kft**., az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

**A Társaság,** az adatkezelő **az adatkezelés tárgyát képező személyes adatok helyesbítését, kiegészítését az érintett kérésére jelen szabályzat 9.7 fejezete szerint végzi el .**

### A törléshez való jog („az elfeledtetéshez való jog”)

Az érintett jogosult arra, hogy kérésére a Társaság, az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat.

A **MORGEN-RED Kft**., az adatkezelő, pedig **köteles** arra, hogy az érintettre vonatkozó **személyes adatokat indokolatlan késedelem nélkül törölje**, ha az alábbi indokok valamelyike fennáll:

* a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték,
* az érintett visszavonja a **Rendelet** 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja,
* az érintett a **Rendelet** 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen
* a személyes adatokat jogellenesen kezelték,
* a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell,
* a személyes adatok gyűjtésére a **Rendelet** 8. cikk (1) bekezdésében említett, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

**Ha a Társaság, az adatkezelő nyilvánosságra hozta** a személyes adatot, és a fentiek szerint azt **törölni köteles**, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, **hogy tájékoztassa az adatokat kezelő adatkezelőket**, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

A **Rendelet** 17.cikk (1) és (2) bekezdés **nem alkalmazandó**, amennyiben az adatkezelés szükséges:

* a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából,
* a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából,
* a **Rendelet** 9. cikk (2) bekezdése h) és i) pontjának, valamint a 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján;
* a **Rendelet** 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az (1) bekezdésben említett jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést, vagy
* jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

## Az adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére a Társaság, az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

* az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát,
* az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,
* az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy
* az érintett a **Rendelet** 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés a fentiek alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

A **MORGEN-RED Kft**., az adatkezelő az **érintettet**, akinek a kérésére **Rendelet** 18. cikk (1) bekezdése alapján korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról **előzetesen tájékoztatja**. Hasonlóan a Társaság, az adatkezelő minden olyan címzettet **tájékoztat** a **Rendelet** 16. cikk, a 17. cikk (1) bekezdése, illetve a 18. cikk szerinti valamennyi helyesbítésről, törlésről vagy **adatkezelés-korlátozásról**, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

## Az adathordozhatósághoz való jog

Az **érintett jogosult arra**, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat **tagolt, széles körben használt, géppel olvasható formátumban megkapja**, továbbá jogosult arra, hogy ezeket az adatokat egy **másik adatkezelőnek továbbítsa** anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

* az adatkezelés a **Rendelet** 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja szerinti hozzájáruláson, vagy a 6. cikk (1) bekezdésének b) pontja szerinti szerződésen alapul, és
* az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

A **Rendelet** 20. cikk (1) bekezdésében említett jog gyakorlása nem érintheti hátrányosan mások jogait és szabadságait, és nem sértheti a 17. cikket. Az említett jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

## A tiltakozáshoz való jog és automatizált döntéshozatal egyedi ügyekben

### A tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a **Rendelet** 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben a Társaság, az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

**Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.**

Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

A **Rendelet** 21.cikk (1) és (2) bekezdésben említett jogra a Társaságnak, az adatkezelőnek, legkésőbb az érintettel való **első kapcsolatfelvétel során kifejezetten** **fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.**

Az információs társadalommal összefüggő szolgáltatások igénybevételéhez kapcsolódóan és a 2002/58/EK irányelvtől eltérve az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

Ha a személyes adatok kezelésére a **Rendelet** 89. cikk (1) bekezdésének megfelelően tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

### Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást

**A Rendelet** 21.cikk (1) bekezdése szerint a**z érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.** Amely nem alkalmazandó abban az esetben, ha a döntés:

* az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
* meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít, vagy
* az érintett kifejezett hozzájárulásán alapul.

A **Rendelet** 21.cikk (2) bekezdés a) és c) pontjában említett esetekben az adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

A **Rendelet** 21.cikk (2) bekezdésben említett döntések nem alapulhatnak a személyes adatoknak a **Rendelet** 9. cikk (1) bekezdésében említett különleges kategóriáin, kivéve, ha a **Rendelet** 9. cikk (2) bekezdésének a) vagy g) pontja alkalmazandó, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

## Az érintetti kérelmek kezelése

A **MORGEN-RED Kft.** vezetősége döntése alapján, a belső adatvédelmi felelős felelős azért, hogy a Társaság mint adatkezelő indokolatlan késedelem nélkül, de minimálisan az érintetti kérelem beérkezésétől számított 30 napon (1 hónap) belül tájékoztatja az érintett magánszemélyt a jogai gyakorlására irányuló kérelmében foglaltak teljesítéséről, a kérelem esetleges elutasításáról és a jogorvoslati lehetőségekről.

Érintetti kérelem alapján történő eljárás esetén az **adatigénylő személyazonosító adatai** csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez - beleértve az esetleges költségek megfizetését is - **elengedhetetlenül szükséges**. A kérelem teljesítését, illetőleg a költségek megfizetését követően az igénylő személyes adatait haladéktalanul törölni kell, amennyiben erről más jogszabály, különösen a Számvitelről szóló 2000. évi C. törvény másként nem rendelkezik.

Az érintett magánszemélynek, személy azonosítása mellett lehetősége van bármely általa választott módon **kérelmet benyújtani** a Társasághoz, az adatkezelőhöz **személyesen, postai úton, elektronikus levélben, meghatalmazott útján,** illetve egyéb módon.

A belső adatvédelmi felelős átvizsgálva a beérkezett kérelmet, és annak teljesítésének nem látva akadályát, úgy azt 30 napon belül teljesíti, majd erről értesíti az érintettet. A kérelem teljesítésének módja lehetőség szerint az érintett által igényelt mód:

* tájékoztatási kérelem esetén: e-mail-ben, postai úton, személyesen,
* adatpontosítás és korlátozási kérelem esetén a tárolt adatra vonatkozó belső végrehajtással,
* adattörlésre vonatkozóan az adat törlésével,
* adattovábbítás, adathordozás esetén az átadással (CD, DVDD átadása, e-mail útján, személyesen)
* tiltakozásnak helyt adó kérelem esetén a kívánt állapot létrehozásával.

Amennyiben a belső adatvédelmi felelős úgy ítéli meg, hogy az érintett magánszemély **kérelmének teljesítésére nincs lehetőség, úgy a kérelem elutasításáról és a jogorvoslati jogokról tájékozatja a kérelmezőt**. A Társaság, az adatkezelő/adatfeldolgozó **jogosult és köteles ellenőrizni a kérelmező személyazonosságát** az adatok bizalmassága és jogi kötelezettségek teljesítése érdekében. Az azonosítás lehetőség szerint az adatmegadás, adatszerzés módjához kapcsolódik.

A Társaság, az adatkezelő/adatfeldolgozó az érintetti kérelmek elbírálása során tevékenységéért költséget, díjazást nem számol fel, de ismételt, megalapozatlan, célszerűtlen kérelmek esetén az ügyintézésre jogosult költség felszámításra. Az átláthatóság miatt minden az érintetti kérelemmel kapcsolatos tevékenységeket Az érintetti kérelmek nyilvántartása dokumentumban rögzíti a belső adatvédelmi felelős.