ADATKEZELÉSI SZABÁLYZAT

EWG Rail Zrt.
Hatályos: 2024. 08. 30.

Bevezetés

Az EWG Rail Zártkörűen Működő Társaság (Cg.01-10-049688; adószám: 26242387-2-41. a továbbiakban: Társaság vagy Adatkezelő) elkötelezett a munkatársai és üzleti partnerei, valamint vele kapcsolatba kerülő harmadik személyek, ideértve a https://ewgrail.com/ honlap látogatóit is, (továbbiakban: Érintettek) személyes adatainak védelme érdekében, kiemelten fontosnak tartja az önrendelkezési jog tiszteletben tartását. A jelen Adatkezelési Utasítás és különösen az ebben foglalt szabályozások és eljárásrendek megalkotásának célja annak biztosítása, hogy az Adatkezelő megfeleljen az adatvédelemmel kapcsolatos hatályos nemzetközi és hazai jogszabályi előírásoknak különösen az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) (a továbbiakban: „GDPR") valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: "Info tv."). Az Adatkezelő valamennyi adatkezelése során jelen adatkezelési szabályzat (a továbbiakban: Adatkezelési Szabályzat), továbbá egyéb belső szabályzatai, utasításai rendelkezései szerint jár el. A jelen Adatkezelési Szabályzatot évente kötelező felülvizsgálni, és a vonatkozó jogszabályi rendelkezéseknek való megfelelést ellenőrizni. A jelen Adatkezelési Szabályzat tartalmáért, betartásáért és a folyamatok megfelelő kialakításáért az ügyvezetés felel.

Kinek kell betartania ezt a szabályzatot?

Jelen szabályzatot a Társaság munkavállalói, a Társaságnál munkavégzésre irányuló egyéb jogviszonyban álló személyek és a Társaság által megbízott adatfeldolgozók kötelesek betartani, és munkájukat a szabályzatban foglaltak alapján kötelesek végezni.

FŐBB VONATKOZÓ JOGSZABÁLYOK

Adatkezelőnek az adatkezelése során az alábbi jogszabályokban foglalt előírásoknak megfelelően kell eljárnia, a jelen szabályzatban foglaltak szerint:

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (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) (továbbiakban: **GDPR**)

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: **Info tv.**)

2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: **Ptk.**)

2012. évi C. törvény a Büntető Törvénykönyvről (továbbiakban: Btk.)

2012. évi I. törvény a Munka Törvénykönyvértől (továbbiakban: **Mt.**)

2012. évi XLI. törvény a személyszállítási szolgáltatásokról (továbbiakban: **Személyszállítási tv.**)

1997. évi CLV. törvény a fogyasztóvédelemről (**Fgy. tv.**)

2000. évi C. törvény a Számvitelről (továbbiakban: **Számviteli tv.**)
2017. évi LIII. törvény a Pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról (továbbiakban: **Pmt.**)
2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (továbbiakban: **Szvmt.**)

A SZABÁLYZAT CÉLJA

A Társaság a jelen Adatkezelési Szabályzatban rögzített szabályozások alkalmazása és betartása/betartatása útján, a jelen Adatkezelési Szabályzatra épülő belső utasításokkal és eljárásrendekkel tudja biztosítani a vonatkozó jogszabályokban, így különösen a GDPR-ban rögzített előírások gyakorlatban való érvényesülését. Ennek keretében a Társaság a jelen Adatkezelési Szabályzattal meghatározza azokat a kereteket, melyekkel

- biztosítja az Érintetteknek a személyes adatok védelméhez fűződő alapvető jogai érvényesülését, az adatbiztonsági követelmények betartását, betartatását;
- szabályozza az adatkezelése megtervezésének, a kockázatok értékelésének folyamatát és felülvizsgálatát;
- szabályozza az adatokhoz történő jogosulatlan hozzáférés megakadályozásának gyakorlatát, valamint meghatározza azokat a szabályokat, melyek biztosítják az adatok törvénysértő megváltoztatásának, az adatok jogosulatlan felhasználásának, valamint engedély nélküli nyilvánosságra hozatalának megakadályozását;
- meghatározza az elektronikus úton történő adatkezelés, feldolgozás, felhasználás, továbbítás, megsemmisítés pontos és biztonságos rendjét;
- meghatározza az érintettek tájékoztatására, tájékoztatáshoz fűződő jogainak érvényesítésére vonatkozó eljárásrendeket és kötelező minimális tartalmat;
- meghatározza az adatvédelmi incidens és a hatósági eljárás során követendő szabályokat;
- meghatározza a szervezet adatvédelmi tudatosságának fejlesztése érdekében minimálisan alkalmazandó eljárásokat.

A részletes belső utasításokat és eljárásrendeket a jelen Adatkezelési Szabályzattal összhangban, a tényleges folyamatok figyelemben vételével kell kialakítani és szükség szerint dokumentálni.

1. ÁLTALÁNOS RÉSZ

1.1. ÉRTELMEZŐ RENDELKEZÉSEK

Fogalmak felvezetése a szabályzatok alkalmazása során:

„személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható – tehát minden olyan adat személyes adatnak minősül, ami alapján az érintett azonosítható: név, lakcím, telefonszám, GPS adat, IP cím stb.

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

„adatkezelés”: a személyes adatokon vagy adatállományokon automatizált, vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés – tehát minden olyan tevékenység, ami az adatokkal kapcsolatos: adatok felvétele, adatokban való betekintés, adatok rendszerezése stb.

„adattovábbítás”: a személyes adat egy meghatározott harmadik személy számára történő hozzáférhetővé tétele.

„nyilvánosságra hozatal”: a személyes adat bárki számára történő hozzáférhetővé tétele.

„adattörlés”: a személyes adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

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

„nyilvántartási rendszer”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető

„adatvagyon leltár”: az adatkezelő által kezelt személyes adatok körének és jellegének felmérését szolgáló dokumentum.

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

„**adatfeldolgozó**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel; *adatfeldolgozónak minősül minden olyan személy vagy vállalkozás, aki a Társaság megbízásából és utasításai szerint a személyes adatokkal meghatározott műveleteket végez (bérszámfejtő, tárhely szolgáltató, szoftver szolgáltató, foglalkozás-egészségügyi orvos stb.)*

„**címzett**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak; - *címzettnek minősül minden olyan személy, társaság vagy hatóság, aki részére az adatok továbbításra kerülnek, vagy akik az adatokhoz hozzáférnek: pl. adóhatóság, adatfeldolgozó, munkaerő-közvetítő stb.)*

„**harmadik fél**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak; - *minden olyan személy vagy társaság, aki alapesetben nem hozható összefüggésbe az adatkezeléssel;*

„harmadik ország”: minden, az Európai Gazdasági Térségen kívüli ország.

„**az érintett hozzájárulása**”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez; - *ilyen lehet az írásbeli hozzájáruló nyilatkozat, a honlapon a hozzájárulási checkbox kipipálása stb., fontos tudni, hogy adatvédelmi szempontból a hallgatás nem minősülhet beleegyezésnek)*

„**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; - *minden olyan esemény, ami az adatokat veszélyezteti: pl. hacker támadás, irattár leégése, de ilyennek minősül például az adatokat tartalmazó laptop, mobil telefon, adathordozó elvesztése, személyes adatok rossz e-mail címre küldése, személyes adatok nem biztonságos tárolása (pl. szemetesbe dobott fizetési papírok); adatok nem biztonságos továbbítása, ügyfél- és vevő- partnerlisták illetéktelen másolása stb.)*

„titoksértési incidens”: olyan incidens, amelynek eredményeként a személyes adatok jogosulatlan vagy véletlen közlése vagy az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés következett be.

„sértetlenségi incidens”: olyan incidens, amelynek eredményeként a személyes adatok jogosulatlan vagy véletlen módosítása következett be.

„hozzáférhetőségi incidens”: olyan incidens, amelynek eredményeként a személyes adatokhoz való hozzáférhetőség jogosulatlan vagy véletlen elvesztés vagy jogosulatlan vagy véletlen megsemmisítés miatt következett be.

„adatbiztonság”: minden olyan technikai vagy szervezési intézkedés, amelynek célja a kezelt személyes adatok – fizikai, optikai vagy szervezeti – biztonságának biztosítása, így különösen azok az intézkedések, amelyek a személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet szolgálják.

1.2. AZ ADATKEZELÉS ELVEI

A személyes adatok

- kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”); - ami azt jelenti, hogy az adatokat csak a vonatkozó jogszabályi rendelkezések szerint szabad kezelni, és az érintett részére lehetővé kell tenni, hogy az adatkezelés körülményeiről (céljai, jogalap, időtartam stb.) megfelelően tájékozódhasson;
- gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azokat nem szabad kezelni a meghatározott célokkal össze nem egyeztethető módon (közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés megengedett) („célhoz kötöttség”); - ami azt jelenti, hogy egy meghatározott célból kezelt adatot csak kivételesen lehet más célra is felhasználni;
- az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”); - ami azt jelenti, hogy csak akkor kezelhető a személyes adat, ha nincs más mód a meghatározott cél elérésére;

- 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 („pontosság”); - ami azt jelenti, hogy az adatokban bekövetkező változásokat a lehető leghamarabb át kell vezetni;
- tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; („korlátozott tárolhatóság”); ez azt jelenti, hogy a meghatározott cél elérését (az adatkezelés maximális időtartamát) követően az adatot vagy törölni, vagy anonimizálni kell, hogy az adatból már ne lehessen az érintettet azonosítani;
- 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”); - megfelelő IT és egyéb biztonsági intézkedések kellenek, hogy illetéktelenek ne férjenek hozzá az adatokhoz;
- Az adatkezelő felelős a fentieknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”) – az adatkezelő az adatkezelési folyamatait belső utasításokkal, szabályozásokkal rögzíti, hogy a szervezetben pontosan követhetők legyen a folyamatok (és szükség esetén ez igazolható legyen a hatóságok felé).

1.3. AZ ADATKEZELÉS CÉLJAI ÉS JOGALAPOK

Adatkezelések céljai

Az adatkezelések célját a Társaság minden egyes adatkezelés esetén külön határozza meg az adatkezelés megkezdését megelőzően.

Általános jelleggel elmondható, hogy az Érintettek adatait a Társaság üzleti működésével összefüggő tevékenysége, szerződéses jogai és kötelezettségei érvényesítése érdekében kezeljük.

Adatkezelések jogalapja

Az adatkezelések jogalapját a Társaság szintén minden egyes adatkezelés esetén külön határozza meg.

A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül: a) Az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez:

Az érintett hozzájárulása minden esetben önkéntes, és kizárólag valamilyen aktív cselekménnyel valósulhat meg (a hallgatás nem beleegyezés). Ilyen lehet az írásbeli hozzájárulás (akár külön

nyilatkozatban, akár például egy szerződés aláírásával, ahol a szerződés maga tartalmazza a hozzájárulást), az elektronikus felületen történő checkbox kipipálás, „hozzájárulok” gombra kattintás stb.).
A hozzájárulást minden egyes adatkezelés tekintetében külön-külön kell/lehet megadni.
Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelések jogszerűségét, tehát a hozzájárulást csak a jövőre nézve lehet visszavonni. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását, tehát a hozzájárulás visszavonása történhet akár egy írásbeli levél formájában, továbbá telefonon, e-mail-ben megküldött nyilatkozat formájában is.

16 évet be nem töltött személy, illetve a cselekvőképességében korlátozott személy hozzájáruló jognyilatkozata akkor érvényes, ha azt a gyermek feletti szülői felügyeletet gyakorló/illetve cselekvőképességében korlátozott személy esetén gyámja/gondnoka adta meg. Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

Az érintett hozzájárulása akkor tekinthető az adatkezelés érvényes jogalapjának, amennyiben az az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

Az érintett hozzájárulása során biztosítani kell azt, hogy valódi választási lehetőség álljon az érintett rendelkezésére, a beleegyezés „tudatossága” felől nem lehet kétség.
Nem minősül önkéntesnek a hozzájárulás akkor, ha annak következményei aláássák az egyén választási szabadságát.

Az érintett hozzájárulása esetén továbbá:

- az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult;
- az Adatkezelőnek biztosítania kell azt, hogy az érintett a hozzájárulását bármikor visszavonhassa, és a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tennie, mint annak megadását;
- a hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak;
- 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;
- nem tekinthető önkéntesnek a beleegyezés, ha nem tesz lehetővé külön-külön hozzájárulást a különböző személyes adatkezelési műveletekhez;
- nem tekinthető önkéntesnek a hozzájárulás, ha a szerződés teljesítését (például a szolgáltatás nyújtását) olyan adatkezeléshez való hozzájárulásához kötik, amely adatkezelés nem szükséges a szerződés teljesítéséhez;

- a hozzájárulás nem szolgálhat érvényes jogalapként akkor, ha az érintett és az Adatkezelő között egyértelműen egyenlőtlen viszony áll fenn;
- ha az Adatkezelő írásbeli nyilatkozaton keresztül szerzi be az érintett hozzájárulását, akkor a nyomtatványon a hozzájárulás iránti kérelmet egyértelműen és világosan el kell választani a szerződés többi részétől, valamint ezen kérelmet érthető és egyszerű nyelvezettel kell az adatkezelőnek megfogalmaznia.

A hozzájárulás beszerzése előtt az Adatkezelő, az Adatkezelővel munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló személy, vagy az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozó köteles megfelelő tájékoztatásban részesíteni az érintettet. A tájékoztatás megtörténhet az erre rendszeresített hozzájáruló nyilatkozaton feltüntetett információk megismerése révén. Ebben az esetben elegendő időt kell biztosítani az érintett számára arra, hogy megismerje a tájékoztatást és megértse a benne foglaltakat.

Az érintett jogosult további információkat és felvilágosítást kérni az Adatkezelőtől, az Adatkezelővel munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló személytől, vagy az Adatkezelővel kötött szerződés alapaján eljáró adatfeldolgozótól. A tájékoztatás vagy felvilágosítás megadása kötelező.

b) 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 (szerződéses kötelezettség):
Amennyiben a személyes adat kezelése nélkül a szerződés teljesítése nem lehetséges, úgy ez jogszerű indoka lehet az adatkezelésnek. Ilyen esetben nem szükséges az érintett külön hozzájárulása.
A szerződések teljesítése körében felmerülő adatkezelések leggyakrabban a szerződő felek szerződésben rögzített személyes adataira vonatkoznak (név, lakcím stb.), de ilyenek lehetek például egy szolgáltatás igénybevétele esetén a szolgáltatás igénybevételével összefüggő adatok. Ilyen például amikor egy vásárlás során a vevő részére névre szóló számlát állítunk ki.

A szerződés megkötése érdekében akkor kezelhetők személyes adatok, ha:
- a szerződést az Adatkezelő köti az érintettel;
- az érintett bocsátja az adatokat az Adatkezelő rendelkezésére;
- az adatok az Adatkezelő és az érintett közötti szerződés megkötéséhez szükségesek.

A szerződés teljesítése érdekében akkor kezelhetők a személyes adatok, ha:
- létezik a szerződés, amelynél az érintett az egyik fél;
- a szerződés érvényes;
- az adatkezelés ténylegesen szükséges a szerződés általános célkitűzésének eléréséhez.

A szükségesség követelménye a szerződéses jogalap alkalmazásának előfeltétele. E követelmény nem redukálható pusztán a szerződéses kitételek vizsgálatára, hanem feltételezi az adatvédelmi garanciák, illetve a GDPR-ban meghatározott alapelvek mérlegelését is, különös tekintettel a tisztességes eljárás, a célhoz kötöttség és az adattakarékosság elvére. Amennyiben tehát az adatkezelés hasznos, de nem objektíve szükséges a szerződés teljesítéséhez, nem alkalmazható a szerződéses jogalap.

c) az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges (jogszabályi kötelezettség)

A jogi kötelezettség teljesítése abban az esetben szolgáltathat jogalapot a személyes adatok kezeléséhez, amennyiben:

- azt uniós vagy hazai jogszabály rendeli el;
- a rendelkezés közvetlenül az Adatkezelőre vonatkozó kötelezettséget tartalmaz;
- a rendelkezés közérdekű célt szolgál;
- a rendelkezés arányos az elérni kívánt jogszerű céllal.

A jogszabályokon alapuló adatkezelések célja az adott jogszabályban foglalt kötelezettségek teljesítése. A jogszabályban elrendelt adatkezelések kötelező adatkezeléseknek minősülnek, melyek mértékét és időtartamát minden esetben a vonatkozó jogszabályok határozzák meg. Nagy számú jogszabály ír elő adatkezelési kötelezettséget. Fontos, hogy a jogszabályi kötelezettség nem opcionális, tehát azokat minden esetben teljesíteni kell. Ilyenek lehetnek például az adózási, bérszámfejtési kötelezettségekkel összefüggő adatkezelések, a kötelező munkaköri alkalmassági vizsgálatokkal összefüggő adatkezelések, jótállási/szavatossági igények intézése során felvett jegyzőkönyvek stb.) A vonatkozó jogszabályi szakaszt minden esetben fel kell tüntetni.

d) Olyan adatkezelések, ahol az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges

Olyan speciális esetben, amikor az érintett nem tudja a saját érdekeit érvényesíteni, vagy az eljárásában akadályoztatva van, lehetőség van arra, hogy az adatai kizárólag a szükséges mértékben, és kizárólag az akadályoztatás idejére a létfontosságú érdek érvényesítése körében kerüljön kezelése.

e) Olyan adatkezelések, ahol az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (hatósági adatkezelések) Miután a Társaság nem hatóság, így ilyen jogalapon nem végez adatkezelést.

f) Olyan adatkezelések, ahol az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges (jogos érdek), 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

Az Adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre, feltéve, hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait.

Az Adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke nem teremthet jogalapot az adatkezelésre, amennyiben az adatkezelést az Adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél közfeladat ellátásával összefüggésben végzi.

A jogos érdek fennállásának megállapításához megvizsgálandó többek között az, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor.
Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az Adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számítanak további adatkezelésre.

A jogos érdek jogalapként történő kezeléséhez az szükséges, hogy az Adatkezelő elvégezze az ún. érdekmérlegelési tesztet. Az érdekmérlegelési teszt a következő lépésekből áll:

- meg kell határozni az adatkezelő jogszerű, egyértelmű és valós érdekét;
- azonosítani kell az érintett alapvető jogait és szabadságait, valamint figyelembe kell venni az érintett elvárásait;
- elemezni kell az adatkezelés szükségességét és arányosságát;
- további olyan intézkedéseket kell meghatározni, amelyek az adatkezelés hatásait csökkentik.

Az érdekmérlegelési tesztet a Társaság minden esetben írásban dokumentálja, annak megállításairól pedig az Érintett tájékoztatást kérhet.
Az Érdekmérlegelési Teszt részletes leírását a 2.1 pont tartalmazza.

1.4. AZ ÉRINTETTEK ADATKEZELÉSSEL ÖSSZEFÜGGŐ JOGAI

Előzetes tájékoztatási kötelezettség

Az érintettek részére a személyes adatok megszerzésének időpontjában tájékoztatást kell adni a személyes adatok kezelésének tényéről, céljáról, jogalapjáról, a kezelt adatok köréről, az adatkezelés módjáról, időtartamáról vagy az időtartam meghatározásának szempontjairól, az adattovábbítás szabályairól, a felügyeleti hatósághoz címzett panasz benyújtásának jogáról.

Az előző bekezdés szerinti tájékoztatás mellett az érintett figyelmét kifejezetten fel kell hívni a tiltakozáshoz való jog érvényesítésének lehetőségére, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

A tájékoztatást:

a) az álláspályázatot benyújtók számára az álláspályázati felhívás közzétételét szolgáló oldalon a vonatkozó adatkezelési tájékoztató szerinti tartalommal kell nyújtani;

b) az Adatkezelővel munkaviszonyt, munkavégzésre irányuló egyéb jogviszonyt létesítő személyek részére a jogviszony létrejöttekor a vonatkozó adatkezelési tájékoztatók szerinti tartalommal kell nyújtani;

Az a) pont szerinti tájékoztatást az Adatkezelő honlapján, tömör, átlátható, és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell elhelyezni.

A b) pont szerinti tájékoztatást a jogviszony létesítésekor elektronikus formában kell megadni, melynek megtörténtét az érintett papír alapú nyilatkozatával írásban igazolni köteles.

Az érintett hozzáférési joga

Az érintett kérelmére az adatkezelést végző illetékes ügyintéző a kérelem beérkezésétől számított 30 napon belül tájékoztatást ad az érintett vonatkozásában folyamatban lévő adatkezelésről.

Az érintett jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;

b) az érintett személyes adatok kategóriái;

c) 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;

d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

e) 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;

f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;

g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ.

A személyes adatokhoz való hozzáférést úgy kell biztosítani, hogy ez alatt az érintett más személy személyes adatait lehetőleg ne ismerhesse meg. Ez alól kivételt képezhetnek azok a személyes adatok, amelyek mind az érintettre, mind pedig egy másik személyre vonatkoznak.

Az érintett hozzáféréshez való jogát az Adatkezelő az elérni kívánt céllal arányosan korlátozhatja vagy megtagadhatja, ha ezen intézkedés elengedhetetlenül szükséges:

a) az Adatkezelő részvételével végzett vizsgálatok vagy eljárások – így különösen büntetőeljárás – hatékony és eredményes lefolytatásának;

b) bűncselekmények hatékony és eredményes megelőzésének és felderítésének;

c) bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtásának;
d) a közbiztonság hatékony és eredményes védelmének;
e) az állam külső és belső biztonsága hatékony és eredményes védelmének, így különösen honvédelem és nemzetbiztonság; vagy
f) harmadik személyek alapvető jogai védelmének biztosításához.

Amennyiben az Adatkezelő a fentiek szerint megtagadja vagy korlátozza az érintett hozzáférési jogát, erről haladéktalanul írásban tájékoztatja érintettet – amennyiben a korlátozás, megtagadás célját ez nem veszélyezteti – az intézkedés indokát is megjelölve. A tájékoztatásban az Adatkezelő külön felhívja érintett figyelmét, hogy hozzáférési jogát a felügyeleti hatóság közreműködésével is gyakorolhatja.

Az Adatkezelő a Szabályzat … számú mellékletét képező nyilvántartásban tartja nyilván a hozzáféréshez való jog gyakorlásával kapcsolatos intézkedéseit. Amennyiben az Adatkezelő az Érintett hozzáféréshez való jogát korlátozza vagy megtagadja, az intézkedés jogi és ténybeli indokait is megjelöli.

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.

Az érintett kérelmére az adatkezelést végző illetékes ügyintéző indokolatlan késedelem nélkül helyesbíti az érintettre 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 is.

Az Adatmódosításról minden olyan címzettet tájékoztatni kell, akivel, illetve amellyel a személyes adat közlésre került, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére tájékoztatást kell adni ezen címzettekről.

A törléshez való jog („az elfeledtetéshez 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, ha az alábbi indokok valamelyike fennáll:

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték (megvalósult az adatkezelés célja)
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

- az adatkezelés jogalapja az adatkezelő jogos érdeke és az érintett tiltakozik az adatkezelések ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett tiltakozik a közvetlen üzletszerzést célzó adatkezelés ellen;
- a személyes adatokat jogellenesen kezelték;
- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell (pl. ha hatóság előírja).

Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és azt a fentiek szerint 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.

Az Adatkezelő nem köteles az adatokat törölni, ha az adatkezelés szükséges

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
- a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó jogszabály szerinti kötelezettség teljesítése céljából;
- bizonyos esetekben a népegészségügy területét érintő közérdek alapján;
- közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben törlés valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ennek a célnak az elérést;
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

Az Adattörlésről minden olyan címzettet tájékoztatni kell, akivel, illetve amellyel a személyes adat közlésre került, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére tájékoztatást kell adni ezen címzettekről.

Az adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére 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 (*tehát amíg nem nyer bizonyosságot, hogy a kezelt adatok helyesek*);
- az adatkezelés jogellenes, az érintett azonban ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását (*mer utóbb esetleg az adatkezelés jogszerűvé tehető és akkor nem kell újra felvenni az adatokat*);
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;

- az érintett tiltakozott a jogos érdeken alapul 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 szerint korlátozásra kerül, 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 fontos közérdekéből lehet kezelni. Az adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell.

Az Adatkezelés korlátozásáról minden olyan címzettet tájékoztatni kell, akivel, illetve amellyel a személyes adat közlésre került, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére tájékoztatást kell adni ezen címzettekről.

Az adathordozhatósághoz való jog

Az érintett kérelmére az adatkezelést végző illetékes ügyintéző biztosítja a személyes adatok hordozhatóságát az alábbi feltételek teljesülése esetén:

a) a személyes adatokat az érintett bocsátotta az Adatkezelő rendelkezésére;

b) az adatkezelés jogalapja hozzájárulás vagy az érintett és az Adatkezelő között kötött szerződés;

c) adatkezelés automatizált módon történik;

d) a személyes adatok hordozása nem érinti hátrányosan mások jogait vagy szabadságait.

Az adathordozhatósághoz való jog gyakorlása során az Adatkezelő köteles a személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban az érintett rendelkezésére bocsátani (PDF/XML).

Az érintett kérheti, hogy az Adatkezelő a személyes adatokat közvetlenül egy másik adatkezelő részére továbbítsa. E lehetőséggel az érintett abban az esetben élhet csak, ha az technikailag megvalósítható. Az Adatkezelő emellett – a hozzáféréshez való jog érvényesülésének elősegítése érdekében – papír alapon is köteles rendelkezésre bocsátani a személyes adatokat.

A tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a közérdekből történő, vagy a Társaság jogos érdekén alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben 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 (pl. marketing, hírlevél stb.) 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 felügyeleti hatósághoz címzett panasz benyújtásának joga

Az egyéb közigazgatási vagy bírósági jogorvoslatok sérelme nélkül, minden érintett 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 a GDPR rendelkezéseit.
A panasz tárgyát a felügyeleti hatóság kivizsgálja és ésszerű határidőn belül tájékoztatja a panaszost a vizsgálattal kapcsolatos fejleményekről és eredményekről, különösen, ha további vizsgálat vagy egy másik felügyeleti hatósággal való együttműködés válik szükségessé. A panasz nyomán a felügyeleti hatóság jogosult eljárást kezdeményezni az adatkezelővel szemben.

Ha az adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

A magyar felügyeleti hatóság pontos elérhetősége az Adatkezelési Szabályzatban került feltüntetésre.

Korlátozások

Az Adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel bizonyos esetekben korlátozhatja az érintettek fentiek szerint meghatározott jogait.

2. ELJÁRÁSI UTASÍTÁSOK

2.1. Érdekmérlegelési teszt

Minden esetben, amikor az adatkezelés jogalapja a Társaság jogos érdeke, érdekmérlegelési tesztet kell végezni, és az eredményét megfelelően dokumentálni kell. Az Érdekmérlegelési Teszt nyomtatványa a jelen Adatkezelési Utasítás 1. számú mellékletét képezi.

2.1.1 Az Érdekmérlegelési Teszt lépései

1. **lépés:** Az adatkezelés céljának megállapítása

Személyes adatot kezelni kizárólag előre meghatározott, jogszerű célból lehet. Tilos, az ún. „készletező” adatkezelés, amikor az adatokat előre nem meghatározott célra gyűjtik. Az adatkezelés célját világosan és érthetően kell rögzíteni.

2. **lépés:** A jogos érdek világos meghatározása

Az adatkezelés jogalapjaként alkalmazandó jogos érdeket pontosan, világosan kell meghatározni, olyan részletességgel, hogy összevethető legyen az érintettek alapvető jogaival és szabadságaival. A jogos érdeknek az Adatkezelő által érvényesített érdeknek kell lennie, ami megfelel a jelenlegi tevékenységének. A túl homályos, vagy elméleti érdekek nem megfelelőek.

Azaz, a jogos érdeknek

- törvényesnek kell lennie (azaz feleljen meg az uniós és/vagy a nemzeti jogszabályoknak);
- kellően egyértelműnek (vagyis kellően pontosnak) kell lennie annak érdekében, hogy az érdekmérlegelés tesztet el lehessen végezni az érintettek érdekeire és alapvető jogaira vonatkozóan;
- valós és fennálló érdeknek kell lennie (vagyis nem lehet elméleti érdek).

Jogos érdeknek minősül különösen:

- közvetlen üzletszerzés, piackutatás
- jogi igényérvényesítés, ideértve a peren kívüli eljárások útján történő követelésbehajtást
- csalás, szolgáltatásokkal való visszaélés vagy pénzmosás megelőzése
- dolgozók ellenőrzése
- fizikai biztonság, informatikai és hálózati biztonság elősegítése

3. **lépés:** Annak meghatározása, hogy az adatkezelés feltétlenül szükséges-e az érvényesíteni kívánt érdek eléréséhez

Ezen lépés során azt kell megfontolni, hogy elérhető az adatkezelési cél az adatok kezelése nélkül. Ha igen, akkor az adatkezelés szükségtelen, így az adatkezelést nem lehet végezni. Ha az adatkezelés nélkül a cél nem érhető elé, akkor az érdekmérlegelési tesztet folytatni lehet.

4. **lépés:** Annak értékelése, hogy az adatkezelő érdekei felülírják-e az érintettek alapvető jogait vagy érdekeit

Ennek megállapításához az alábbi körülményeket kell figyelembe venni:

- az adatkezelő érdekének jellege (alapvető jog, közérdek, jogszabályban rögzített jog, üzleti érdek);
- az adatkezelés meghiúsulása esetén az adatkezelő, harmadik felek vagy a szélesebb közösség által elszenvedett esetleges sérelmek;
- az adat jellege (bizalmas vagy tágabb értelemben érzékeny-e);
- az érintettek (kiskorú, alkalmazott stb.) és az adatkezelő jogi helyzete (pl.: a gazdasági társaság domináns piaci helyzetben van-e);
- az adatkezelés módja (profilalkotás, emberek széles körét érinti);
- az érintettek azon alapvető jogai és/vagy érdekei, amelyekre hatással lehet;

- az érintettek ésszerű elvárásai;
- az érintettekre gyakorolt hatások összehasonlítva az adatkezelő adatkezelésből származó előnyeivel.

Általánosan fogalmazva: annak kiértékelése, hogy kinek az érdeke fontosabb és miért?

5. **lépés:** Végső mérleg összeállítása a további garanciák figyelembevételével

Az adatkezelés lehetséges hatásait csökkentő intézkedések meghatározása:

- adatminimalizálás (csak a feltétlenül szükséges adatok kezelhetők és az adatokat a cél megvalósulása utáni azonnal törölni kell, a törlési funkciót lehetőleg automatizálni kell)
- technikai és szervezeti intézkedések végrehajtása annak biztosítása érdekében, hogy az adatokat ne lehessen egyénekkel kapcsolatos döntések meghozatalához vagy egyéb intézkedésekhez felhasználni (funkcionális szétválasztás)
- anonimizálási technikák széleskörű használata, adatok összevonása, magánélet védelmét elősegítő technológiák;
- a tiltakozáshoz való jog biztosítása (opt-out).

6. **lépés:** Transzparencia biztosítása – döntés dokumentálása

- Az érdekmérlegelési teszt folyamatát, az egyes lépések során megfontolt körülményeket dokumentálni kell, olyan részletességgel, hogy a döntés megalapozottsága bizonyítható legyen
- Kétség esetén adatvédelmi felelős/szakértő bevonása szükséges
- Amennyiben az adatkezelési tevékenység magas kockázatot jelent az érintettek jogaira és szabadságaira nézve, adatvédelmi hatásvizsgálatot is kell végezni

2.1.2 Az Érdekmérlegelési Teszt eredménye

Az Érdekmérlegelési Tesztet a Társaság minden olyan adatkezelési tevékenysége esetében le kell folytatni, amikor a Társaság jogos érdeke az adatkezelés jogalapja. A mérlegelésnek magában kell foglalnia a Társaság működésének minden sajátosságát.

Minden Érdekmérlegelési Teszt lefolytatását írásban dokumentálni kell.

Az adatkezelésről szóló tájékoztatóban az Érdekmérlegelési Teszt eredményéről az érintettek részére egyszerű, világos és átlátható tájékoztatást kell adni.

2.1.3 Az Érdekmérlegelési Teszt felülvizsgálata

Az Érdekmérlegelési Teszt megállapításait legalább évente egyszer, de az adatkezelési körülmények változásakor minden esetben felül kell vizsgálni.

Ezen túlmenően amennyiben egy érintett tiltakozik az adatkezelés ellen, úgy az általa megjelölt, saját egyéni körülményei figyelembevételével az érdekmérlegelési tesztet az egyedi érintettre vonatkozóan is felül kell vizsgálni, és a tiltakozása elbírálásakor az érdekmérlegelési teszt felülvizsgálatának megállapításairól is tájékoztatni kell.

2.2. KOCKÁZATÉRTÉKELÉS ÉS ADATVÉDELMI HATÁSVIZSGÁLAT

Az adatvédelmi kockázatértékelés, valamint az adatvédelmi hatásvizsgálat arra ad megoldást, hogy az egyes adatkezelésekkel kapcsolatban hogyan kell beazonosítani a lehetséges kockázatokat, és amennyiben kötelező, hogyan kell teljesíteni az adatvédelmi hatásvizsgálatot, és hogyan kell kezelni a kockázatokat.

A nemzeti adatvédelmi hatóság állásfoglalást adott ki arra vonatkozóan, hogy milyen tevékenységek esetén kötelező az adatvédelmi hatásvizsgálat. Az aktuális lista a NAIH honlapján elérhető, minden egyes adatkezelés tervezésekor ezt a listát ellenőrizni kell.

A kockázatok felmérése és értékelés során, mint minden hasonló eljárás esetén, józan észen alapuló megközelítés, és az általános célkitűzések teljes megértése szükséges, ami nem más, mint a személyes adatok lehető legteljesebb körű védelme és a GDPR követelményeinek való megfelelés.

A GDPR szerint, az Adatvédelmi Hatásvizsgálat követelményeinek való megfelelés elmulasztása esetén a felügyeleti hatóság bírságot szab ki. Az adatvédelmi hatásvizsgálat elmulasztása olyan esetben, amikor az kötelező lenne (35. Cikk (1) és (3-4)), valamint az adatvédelmi hatásvizsgálat nem megfelelő megvalósítása (35. Cikk (2) és (7), (9)), továbbá a felügyeleti hatósággal való előzetes konzultáció elmulasztása 10M euróig terjedő adminisztrációs bírságot eredményezhet, illetve vállalkozások esetén a bírság a megelőző pénzügyi év teljes világszintű éves forgalmának 2%-ig terjedhet, a kettő közül a magasabb bírság alkalmazandó.

A kockázatértékelés eljárására vonatkozó diagram a jelen Adatvédelmi Utasítások 2. számú mellékletét képezi.

2.2.1 A szükségesség és a körülmények meghatározása

A GDPR-ban meghatározott kockázatalapú megközelítéssel összhangban hatásvizsgálat nem kötelező minden egyes adatkezelés esetében. Hatásvizsgálatra csak akkor van szükség, amikor a személyes

adatok kezelése valószínűsíthetően „magas” kockázattal jár a természetes személyek jogaira és szabadságaira nézve (GDPR 35. Cikk (1)). Önmagában az, hogy a hatásvizsgálat lefolytatásának kötelezettségére vonatkozó feltételek nem állnak fenn, nem csökkenti az általános kötelezettséget arra vonatkozóan, hogy az érintettek jogait és szabadságait veszélyeztető kockázatok beazonosítására és megfelelő kezelésére a szükséges intézkedéseket meg kell hozni, ez a kockázatértékelés. A gyakorlatban ez azt jelenti, hogy folyamatosan vizsgálni kell a személyes adatokat érintő adatkezelési tevékenység során felmerülő kockázatokat.

Az adatvédelmi hatásvizsgálatot/kockázatértékelést az adatkezelést megelőzően kell lefolytatni, amely az adatkezelés tekintetében a döntéshozatalt segítő eszköznek minősül.

Az adatvédelmi hatásvizsgálatot/kockázatelemzést mielőbb meg kell kezdeni az adatkezelési művelet kialakítása során, még akkor is, ha az adatkezelés egyes működési elemei nem ismertek.
Az adatkezelési hatásvizsgálat/kockázatértékelés folyamatos kiigazítása a projekt életciklusa alatt biztosítja az adatok megfelelő védelmét, valamint olyan megoldásokra ösztönöz, amelyek elősegítik a GDPR megfelelést.

A fejlesztési folyamatok előre haladtával a vizsgálat egyes lépéseinek ismétlése szükségessé válhat, mert bizonyos technikai vagy szervezeti intézkedések hatással lehetnek az adatkezelés során felmerült kockázatok súlyosságára vagy valószínűségére. A hatásvizsgálat/kockázatértékelés egy folyamatos kötelezettség, különösen azokban az esetekben, ahol az adatkezelési műveletek dinamikusan változnak.

Az a tény, hogy a hatásvizsgálati eljárást/kockázatértékelést esetleg módosítani kell, amikor az adatkezelés ténylegesen megkezdődött, az nem kellő indok arra, hogy a vizsgálat elhalasztásra, vagy leállításra kerüljön. A hatásvizsgálat/kockázatértékelés tehát nem egyszeri feladatot jelent, hanem folyamatos tennivalót.

Számos feltétel számbavétele szükséges annak megállapításához, hogy a Társaság köteles-e lefolytatni adatvédelmi hatásvizsgálatot.

A GDPR (35. Cikk) előírása szerint hatásvizsgálatra van szükség különösen azokban az esetekben, amikor a tervezett adatkezelés során az alábbiakra kerülhet sor:

- 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 (például: munkavállalók tevékenységének módszeres ellenőrzése beleértve a munkavállalók munkahelyét, internet aktivitását stb.)

- a 9. cikk (1) bekezdésében említett személyes adatok különleges kategóriái, vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése;
- nyilvános helyek nagymértékű, módszeres megfigyelése (például: közösségi média adatok összegyűjtése profilok létrehozására)

Megjegyzés: A 9. Cikk (1) bekezdése olyan személyes adatok kezelésére hivatkozik, amelyek a faji vagy etnikai származásra, politikai véleményre, vallási és filozófiai meggyőződésre vagy szakszervezeti tagságra utalnak, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkoznak.

A fenti felsorolás nem kimerítő, az adott körülményektől függően előfordulhatnak további “magas” kockázatot jelentő adatkezelések, amelyeket a fenti felsorolás nem tartalmaz.

Általában a Társaság határoz arról, hogy az adatvédelmi hatásvizsgálatra az adott projekt tekintetében szükség van-e, figyelembe véve a NAIH által közzétett listát, valamint az alábbi egy vagy több feltétel fennállását:

a) személyes adatok megosztásra kerülnek olyan személyekkel, szervezetekkel, akiknek korábban nem volt hozzáférésük;
b) a már kezelt személyes adatok más célra, vagy más módon kerülnek felhasználásra;
c) új adatkezelési technológia kerül bevezetésre;
d) automatizált döntéshozatal/profilalkotás történik;

Amennyiben nem állapítható meg egyértelműen, hogy egy adott projekt esetében adatvédelmi hatásvizsgálatot kötelező-e lefolytatni, javasolt annak lefolytatása. Az adatvédelmi tisztviselővel – amennyiben van – egyeztetni lehet a pontosítás érdekében, és az adatvédelmi hatósággal is lehetséges a konzultáció. A döntést minden esetben az Ügyvezetés jogosult és köteles meghozni (szakértők bevonásával) abban a kérdésben, hogy szükség van-e hatásvizsgálat lefolytatására vagy nincs, vagy a hatósághoz kell-e fordulni.

Rögzíteni kell a hatásvizsgálat megvalósításának teljes környezetét, és annak magyarázatát, mi indokolta a vizsgálatot. A magyarázatnak tartalmaznia kell a projekt belső és külső körülményeit és fő célkitűzéseit.

Pontosan definiálni kell a vizsgálat hatókörét is, amely kifejezhető a projekt meghatározott körülményeivel is, így különösen:

- földrajzi helymeghatározás (pl. ország, iroda, adatközpont)
- szervezeti egységek (pl. meghatározott osztályok)

- üzleti eljárás (ok)
- IT szolgáltatók, rendszerek vagy hálózatok
- ügyfelek, termékek vagy szolgáltatások

Bármilyen kivételt részletesen kell indokolni.

2.2.2 Személyes adatok felhasználásának dokumentálása

A GDPR 35. Cikk (7) a) -b) megállapítja, hogy a hatásvizsgálat kiterjed legalább: a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket; és b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára.

Megfelelő részletességgel kell alátámasztani és dokumentálni, hogy a felhasznált személyes adatok relevánsak a projekt szempontjából, figyelembe véve az alábbiakat:

- A tárolt és adatkezeléssel érintett egyedi adatelemek definíciója
- Annak indokai, hogy az adatkezelés teljes mértékben szükséges és arányos - Az adatkezelés célja és jogalapja
- Hogyan került sor az adatok megszerzésére (adatok forrása)
- Milyen módon kerülnek feldolgozásra az adatok (adatkezelési műveletek, adatfeldolgozók által végzett műveletek)
- Adatok kezelésének időtartama
- Adatok tárolásának módja és helye
- Az adatok esetleges jövőbeni felhasználása
- Adatok továbbítása
- Adatokhoz való hozzáférés

Az információk összegyűjtésére és bemutatására megfelelő információs nyilvántartások, folyamatábrák és adathozzárendelési eszközök által kerülhet sor.

2.2.3 Kockázat-azonosítás

Az összegyűjtött, feldolgozott és tárolt személyes adatokra vonatkozó kockázatok beazonosítása az alábbi lépéseket tartalmazza:

2.2.3.1 Kockázatforrások azonosítása

A kockázatok beazonosítása során az alábbi személyek véleményét kell beszerezni:

Az érintett felek (ahol lehetséges):

- Az érintett tevékenységekért felelős vezető(k)
- A tevékenységet ténylegesen ellátó beosztottak
- A tevékenység inputjáért felelős szolgáltatók
- A tevékenység outputját fogadó személyek
- Releváns ismeretekkel rendelkező, meghatározott harmadik személyek
- A tevékenységhez támogatást és forrásokat biztosító személyek/szervezetek képviselői
- További személyek, akik hasznosan hozzájárulhatnak a kockázatazonosító eljáráshoz

Az azonosított kockázatokat a lehető legrészletesebb leírással kell rögzíteni annak érdekében, hogy a kockázat valószínűsége és hatása értékelhető legyen.

2.2.4 Kockázatelemzés

Az érintettek jogai és szabadságainak változó valószínűségű és összetettségű kockázata a személyes adatok kezeléséből eredhet, amely fizikai, anyagi vagy nem anyagi kárt okozhat. Így különösen az adatkezelés eredményezhet:

- hátrányos megkülönböztetést,
- személyazonosság lopást vagy személyazonossággal való visszaélést, - pénzügyi veszteséget, - jó hírnév sérelmet,
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését,
- üzleti döntések jogosulatlan befolyásolását,
- álnevesítés engedély nélküli feloldását,
- egyéb jelentős gazdasági vagy szociális hátrányt.

A kár eltérő módokon jelenhet meg. Olykor kézzelfogható és számszerűsíthető, mint például a pénzügyi veszteség vagy a munkahely elvesztése. Máskor kevésbé definiálható, így például a bizalmas vagy érzékeny információk kiadása a személyes kapcsolatokban és a szociális helyzetben okoz kárt. Néha a károkozás nem nyilvánvaló, így például a személyazonosság lopástól való félelem, amelynek oka, hogy az információbiztonság veszélybe kerülhet. A személyes információ használatából eredő kár a magánszemélyek számára észlelhetetlen és következmény nélküli is lehet.

Az érintettek jogaira és szabadságaira vonatkozó kockázat valószínűségét és súlyosságát az adatkezelés céljára, jellegére, hatókörére és körülményeire való hivatkozással kell meghatározni.
Az adatbiztonsággal összefüggő kockázatok vizsgálata során figyelembe kell venni azokat a kockázatokat, amelyeket a személyes adatok kezelése jelent, így a véletlen vagy jogellenes megsemmisítést, elvesztést, megváltoztatást, jogosulatlan közlést vagy a személyes adatokhoz való jogosulatlan hozzáférést, továbbá a személyes adatok oly módon történő továbbítását, tárolását vagy egyéb módon való kezelését, amely különösen fizikai, anyagi vagy nem anyagi károkhoz vezethet.

A kockázatelemzés a kockázat a) valószínűségére és b) hatására/súlyosságára nézve számszerű értékeket határoz meg. Ezeknek az értékeknek többszörözésével lehetséges a magas és alacsony kockázatú besorolás megállapítása.

2.2.4.1 A valószínűség értékelése

A kockázat valószínűségére vonatkozóan becslést kell készíteni, amelyhez figyelembe kell venni, hogy korábban a szervezetben vagy hasonló szervezet esetében, ugyanabban a gazdasági ágazatban vagy földrajzi helyszínen előfordult-e korábban az adott kockázat, és hogy elegendő indíték, lehetőség és képesség áll-e fenn a fenyegetettség megvalósulására.

Valamennyi kockázat valószínűségét számszerű egységekben, 1-től 5-ig kell besorolni. A számegységek jelentésére vonatkozó általános útmutatót a következő táblázat tartalmazza. A kockázat-valószínűség értékelésekor figyelembe kell venni a már rendelkezésre álló információkat, belső ellenőrzési eredményeket. A kockázatértékelés tárgyától függően a valószínűség valamennyi szintjére vonatkozóan részletesebb útmutató is alkalmazható.

Szint	**Megnevezés**	**Leírás**
1	Valószínűtlen	Korábban nem történt meg soha, nincs ok azt gondolni, hogy most nagyobb a valószínűsége
2	Nem valószínű	Elképzelhető, hogy megtörténhet, de valószínűleg nem kerül rá sor
3	Valószínű	Összességében valószínűbb, hogy a kockázat felmerül, mint hogy nem merül fel
4	Nagyon valószínű	Meglepő volna, ha a kockázat nem fordulna elő, figyelembe véve a múltbeli gyakoriságot, és a jelenbeli körülményeket
5	Szinte biztos	Vagy rendszeresen előfordul, vagy okkal hihető, hogy közvetlenül fenyegető a kockázat

Rögzíteni kell az adott szint alkalmazásának az indokait az értelmezés elősegítése érdekében, valamint azért, hogy a jövőbeni értékelések során az ismételhetőség lehetővé váljon.

2.2.4.2 A kockázat hatásának/súlyosságának vizsgálata

Értékelést kell készíteni a kockázat hatásáról, amelyet az érintettek jogaira és szabadságaira, valamint a szervezetre gyakorolhat. Figyelembe kell venni hozzá a meglévő, hatékony ellenőrzéseket, amelyek enyhítik a hatást.

Az alábbi területeken kell a hatást mérlegelni:

- Érintettek (többnyire ügyfelek) jogai és szabadságai
- Pénzügyek
- Egészség és Biztonság
- Jó hírnév
- Jogi, szerződéses vagy szervezeti kötelezettségek

Valamennyi kockázat hatását egy számskálán 1 (alacsony) és 5 (magas) között kell jelölni. A következő táblázat tartalmazza valamennyi érték jelentésére vonatkozó általános útmutatót.

A kockázatértékelés tárgya alapján lehetőség van részletesebb iránymutatás meghatározására a hatás minden egyes szintje tekintetében.

Rögzíteni kell az adott szint alkalmazásának indokait az értelmezés elősegítése érdekében, valamint azért, hogy a jövőbeni vizsgálatok során a megismételhetőség lehetséges legyen.

Adott esetben a tervezett adatkezelésről ki kell kérni az érintettek vagy képviselőik véleményét, az üzleti- vagy közérdek védelme, illetőleg az adatkezelési műveletek biztonságának sérelme nélkül.
A véleményeket különböző eszközök útján lehet beszerezni, és a körülményektől függően (pl. az adatkezelési műveletek céljával és eszközeivel kapcsolatos általános tanulmány, a vezetés képviselőihez intézett kérdés, vagy a jövőbeni ügyfeleknek kiküldött szokásos felmérések) biztosítani kell, hogy a Társaság megfelelő jogi alappal rendelkezzen azon adatok kezelésére, amelyek tekintetében a véleményeket bekérik.
Amennyiben az adatkezelésre vonatkozó végleges döntés különbözik az érintettek véleményétől, akkor dokumentálni kell az indokokat az adatkezelés folytatása vagy az azzal való felhagyás tekintetében. Azt is dokumentálni kell, ha a Társaság nem kéri be az érintettek véleményét, mert úgy dönt, hogy az nem helyénvaló, így pl., ha azt megtennék, az a Társaság üzleti tervének titkosságát veszélyeztetné, vagy aránytalan, illetve a gyakorlatban kivitelezhetetlen volna.

Szint	Leírás	Érintettek jogai és szabadságai	Fogyasztói hatás	Pénzügyi hatás	Egészség és biztonság	Hírnévre gyakorolt hatás	Jogi hatás
1	Elhanyagol-ható	Nincs hatása, minden jog és szabadság biztosított	Nincs hatása	Nincs vagy nagyon csekély	Nagyon csekély további kockázat	Elhanyagol-ható	Nincs hatása
2	Enyhe	Enyhe korlátozás	Bizonyos helyi zavarok a szokásos üzletmenetben	Néhány	Elfogadható mértékben	Csekély	Csekély kockázat a kötelezettség elhanyagolása miatt
3	Mérsékelt	A jogok és sza-badságok látható korlátozása, de az adatkezelés célja elsőbbséget élvez a korlátozások-kal szemben	Még lehet terméket szállítani/ szolgáltatást nyújtani némi nehézséggel	Nem kívánatos de elviselhető	Magas kockázat; azonnali fellépést igényel	Mérsékelt	Az illegális működés valós veszélye

Szint	Leírás	Érintettek jogai és szabadságai	Fogyasztói hatás	Pénzügyi hatás	Egészség és biztonság	Hírnévre gyakorolt hatás	Jogi hatás
4	Magas	A magánéletbe való indokolatlan beavatkozás	Súlyos üzleti veszteség a fő területeken	Súlyos hatás a bevételre és /vagy a nyereségre	Jelentős életveszély	Magas	Néhány területen illegális működés
5	Nagyon magas	Az érintett kárt szenved	Gazdasági ellehetetlen-ülés;	Működés-képtelenség	Valós vagy erősen valószínű haláleset	Nagyon magas	Súlyos bírság, kártérítési és büntetőjogi következmények

2.2.4.3 Kockázat besorolása

A valószínűség és a hatás/súlyosság fokának értékelése alapján valamennyi kockázat tekintetében két szám szorzatával egy értéket kapunk meg. A 2. ábrában mutatott mátrix alkalmazásával dönthető el a megkapott érték alapján a kockázat besorolása.

Valamennyi kockázatot az alábbi értékek alapján kell besorolni, a következő táblázat szerint.

MAGAS – 5 vagy több

ALACSONY – 1-4

5	Magas	Magas	Magas	Magas	Magas
4	Alacsony	Magas	Magas	Magas	Magas
3	Alacsony	Magas	Magas	Magas	Magas
2	Alacsony	Alacsony	Magas	Magas	Magas
1	Alacsony	Alacsony	Alacsony	Alacsony	Magas
	1	2	3	4	5

A GDPR előírása szerint hatásvizsgálati eljárásra van szükség abban az esetben, ha az adatkezelés valószínűleg magas kockázatot jelent a természetes személyek jogaira és szabadságaira, vagyis a GDPR csak alacsony és magas kockázatot különböztet meg. Ennek megfelelően, amennyiben

bármelyik adatkezelés értékelésének eredménye 5, vagy attól magasabb érték, abban az esetben hatásvizsgálatot kell lefolytatni.

2.2.5 Kockázat-értékelés

A kockázat értékelés célja annak eldöntése, hogy melyik kockázat elfogadható, és melyeket kell kezelni.

A fenti ábrában jelölt mátrix tartalmazza a kockázat besorolását. A zöld szín jelöli az elfogadható határérték alatti kockázatot. A vörös színű területek általában azt jelzik, hogy a kockázat nem felel meg a kockázat elfogadás kritériumának, és ezért kockázat kezelésre lesz szükség.

2.2.6 Kockázatkezelési terv meghatározása

Azokra a kockázatokra, amelyek a fentiek szerint a Társaság részéről határérték fölöttiként kerültek megállapításra, megoldásokat kell kidolgozni a kockázatok mérséklésére.

A kockázatkezelés általános célja a kockázat besorolásának elfogadható szintre való csökkentése. Ez nem minden esetben lehetséges, mert ugyan néha csökken az érték, mégis a kockázat ugyanabban a besorolásban marad pl. 8-ról 6-ra való értékcsökkenés még mindig magas kockázati értéket jelent. A szervezet eldöntheti, hogy elfogadja ezeket a kockázatokat a magas kockázati szint ellenére. Az ilyen típusú döntéseket megfelelő magyarázattal rögzíteni szükséges.

2.2.6.1 Kockázatkezelési módszerek

Az alábbi módszerek alkalmazhatók azon kockázatok kezelése során, amelyeket elfogadhatatlannak minősítettek.

- Kockázat módosítása – olyan ellenőrzések alkalmazása, amelyek a kockázat valószínűségét és/vagy hatását csökkentik
- Kockázat elkerülése olyan intézkedések bevezetésével, amelyek révén a kockázat már nem létezik
- Kockázat megosztása egy másik partnerrel, (pl. biztosító vagy szállító)

A döntéshozatal során mérlegelni kell a megteendő lépéseket, amelyeknek a kockázattal kapcsolatos körülmények biztos ismeretén kell alapulnia. Így különösen

- Üzleti stratégia
- Szabályozási és jogi megfontolások
- Technikai kérdések
- Kereskedelmi és szerződéses kérdések

2.2.6.2 Ellenőrzések kiválasztása

Megfelelő ellenőrzéseket kell meghatározni annak érdekében, hogy csökkentsék valamennyi kockázat valószínűségét vagy a hatását (vagy mindkettőt) az elfogadható szintre.

2.2.7 Kockázatértékelési/hatásvizsgálat jelentés

Az intézkedési lehetőségek értékelése eredményeként a kockázatértékelésről (és adatvédelmi hatásvizsgálatról) jelentés készül, amely az alábbiakat tartalmazza részletesen

- A javasolt adatkezelési műveleteket és az érintett személyes adatoknak a leírását
- Az adatkezelés célját, beleértve adott esetben az adatkezelő jogos érdekét a GDPR-ban meghatározottak szerint
- Az adatkezelés szükségességének és arányosságának az értékelését
- Az érintettek jogai és szabadságai kockázatai értékelésének az eredményét
- Minden egyes kockázat esetében, hogy javasolt-e elfogadásra vagy kezelésre - Kockázatkezelések prioritási sorrendjét
- Kockázat felelősöket
- Javasolt kockázat-kezelési lehetőségeket
- Ellenőrzés(ek) végrehajtását
- A meghozandó intézkedésekért felelősöket
- Az intézkedések menetrendjét
- Fennmaradó kockázatok mértékét az ellenőrzések végrehajtását követően

A hatásvizsgálati jelentés dokumentálására a NAIH honlapján található program (DPIA) használata javasolt, de nem kötelező.

2.2.8 A vezetés jóváhagyásának beszerzése a megmaradó kockázatok tekintetében

Az adatvédelmi hatásvizsgálat valamennyi stádiumában tájékoztatni kell az ügyvezetés a fejlődésről és a meghozott döntésekről, beleértve az előirányzott fennmaradó kockázat formális elfogadását is. Az ügyvezetés jóváhagyja az adatvédelmi hatásvizsgálati jelentést és mérlegeli, a fennmaradó kockázatokat és ezek ismeretében dönt az esetlegesen további lépésekről.

A végleges jóváhagyást a Társaság dokumentumaiban előírt módon kell jelezni.

2.2.9 Előzetes konzultáció a felügyeleti hatósággal

Amennyiben az adatvédelmi hatásvizsgálat magas kockázatot jelez az azonosított ellenőrzések végrehajtását megelőzően, úgy a GDPR előírja, hogy az adatkezelés megkezdése előtt a felügyeleti hatósággal konzultálni kell. A konzultáció során alábbi információkat kell megadni:

- az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók hatásköreinek részletezése;
- a tervezett adatkezelés céljai és módja;
- az alkalmazandó adatvédelmi ellenőrzések;
- az adatvédelmi tisztviselő elérhetősége (amennyiben van adatvédelmi tisztviselő); - a hatásvizsgálati jelentés másolata;
- egyéb, a felügyeleti hatóság által kért információ

Ha a Hatóság az előzetes konzultáció során arra a megállapításra jut, hogy a tervezett adatkezelés vonatkozásában az arra irányadó jogszabályban meghatározott előírások nem érvényesülnek maradéktalanul - különösen, ha álláspontja szerint az adatkezelő az adatkezeléssel járó kockázatokat nem megfelelően azonosította vagy nem megfelelően mérsékelte -, a feladat- és hatáskörébe tartozó bármely egyéb intézkedés megtétele mellett vagy helyett a feltárt hiányosságok megszüntetésére alkalmas lépéseket határoz meg és azok végrehajtására tesz javaslatot az adatkezelő, illetve - annak tevékenységi körére korlátozva - az adatfeldolgozó részére.
A javaslatot a Hatóság az előzetes konzultáció kezdeményezésétől számított hat héten belül, írásban teszi meg. E határidőt a Hatóság legfeljebb egy hónappal meghosszabbíthatja, ebben az esetben a meghosszabbítás tényéről és indokairól az előzetes konzultáció kezdeményezésétől számított egy hónapon belül tájékoztatja az adatkezelőt, illetve az adatfeldolgozót.

2.2.10 Kockázatkezelési intézkedések alkalmazása

A kockázatkezelési terv elfogadását követően nyomon kell követni és végre kell hajtani a szükséges intézkedéseket a projekt napról-napra való ellenőrzésének a részeként. Ha bármelyik intézkedés késedelmet szenved, vagy nem valósul meg, akkor annak hatását az érintett személyes adat védelmére nézve vizsgálnia kell, és dönteni kell a további intézkedésekről. Amennyiben súlyos a kezeletlen kockázat, akkor annak lényeges kihatása lehet a projekt megvalósíthatóságára.

2.2.11 Kockázatellenőrzés és jelentések

Lehetőség szerint a kockázatellenőrzések hatékonyságát objektív mutatókkal mérni és dokumentálni kell.

2.2.12 Rendszeres felülvizsgálat

A kockázatértékelést évente felül kell vizsgálni rendszeresen sort kell keríteni annak érdekében, hogy az értékelések aktuálisak és az alkalmazott megállapítások és ellenőrzések jogilag érvényesek maradjanak. Szükség esetén soron kívüli kockázatértékelést is kell végezni, amikor a körülmények megváltozása ezt indokolja: pl. jelentős üzleti változások esetén, összeolvadások és akvizíciók, megváltozott IT szolgáltatás/technológia esetén stb.

2.2.13 Szerepek és hatáskörök

A kockázatvizsgálati és ellenőrzési eljárásokban a résztvevők és hatásköreik az adott projekt esetén egyedileg kerülnek meghatározásra minden esetben, igazodva fentiek szerinti folyamathoz. Amennyiben indokolt, úgy adatvédelmi szakértő bevonására is sor kerülhet az ügyvezetés jóváhagyásával.

2.3. ADATKEZELÉSI NYILVÁNTARTÁS

Minden adatkezelő Adatkezelési Nyilvántartást köteles vezetni. Amennyiben az adatkezelő egyes helyzetben adatfeldolgozóként jár el, úgy az Adatkezelési Nyilvántartásnak az adatfeldolgozásokra vonatkozó adatokat elkülönülten kell tartalmaznia. Az Adatkezelési Nyilvántartás formanyomtatványa a jelen Adatkezelési Szabályzat 3. mellékletét képezi. A nyilvántartás vezetéséért az adatvédelmi kapcsolattartó (jelen szabályzat kiadásakor Szontagh Antalné) felelős.

2.4. AZ ADATKEZELŐ ADATVÉDELMI RENDSZERE

SZERVEZETI SZEREPLŐK FELADATAI, HATÁSKÖRE

2.4.1. ADATKEZELŐ

A Szabályzat hatálya alá tartozó adatkezelések tekintetében az EWG Rail Zártkörűen Működő Részvénytársaság minősül adatkezelőnek.

Az Adatkezelőre vonatkozó adatok:

megnevezés:	EWG Rail Zártkörűen Működő Részvénytársaság
rövidített elnevezés:	EWG Rail Zrt.
cégjegyzékszám:	01-10-049688
adószám:	26242387-2-41
székhely:	1134 Budapest, Róbert Károly körút 59.
e-mail:	info@ewgrail.com
telefonszám:	+36 1/866-3080

2.4.2. ADATVÉDELMI TISZTVISELŐ (DPO)

Az adatkezelő és az adatfeldolgozó az alábbi esetekben köteles adatvédelmi tisztviselőt kinevezni:

- ha az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;
- ha 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;
- ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok GDPR 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint az adatvédelmi tisztviselői feladatok ellátására való alkalmasság alapján kell kijelölni.

Az adatvédelmi tisztviselő az adatkezelő vagy az adatfeldolgozó alkalmazottja is lehet, vagy szolgáltatási szerződés keretében egy külsős szolgáltató is elláthatja a feladatokat. Alkalmazott esetén, a Társaság köteles meggyőződni arról, hogy az adatvédelmi tisztviselőnek kinevezett alkalmazottja az adatkezelések egyik lépésében sem vesz részt (függetlenség), azaz nem lehet olyan személy, aki az adatkezelés célját, terjedelmét, szükségességét meghatározza. Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

2.4.3 Adatvédelmi Tisztviselő alkalmazásával összefüggő döntési eljárás

Dokumentálni szükséges az annak eldöntése érdekében készült belső elemzést, hogy a Társaság köteles-e adatvédelmi tisztviselőt kijelölni vagy sem, annak igazolására, hogy a döntéshozatal során a releváns tényezőket megfelelően értékelésre kerültek, kivéve, ha egyértelmű, hogy a szervezet nem köteles adatvédelmi tisztviselőt kijelölni. Mint minden adatvédelemmel kapcsolatos kérdést, ezt a dokumentációt is aktualizálni kell, például, ha olyan új tevékenység, vagy olyan új szolgáltatások merül fel, amelyek a kötelezően alkalmazandó adatvédelmi tisztviselő esetkör hatálya alá tartoznak.

2.4.4 A Társaság jelenlegi döntése az Adatvédelmi Tisztviselő alkalmazásával összefüggésben

A Társaság nem közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv, ezért a GDPR 37. Cikk (1) bekezdés a) pontja nem vonatkozik rá. A Társaság főtevékenysége a személyes adatok GDPR 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, büntetőjogi felelősség megállapítására

vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését nem foglalják magukban, így a GDPR 37. cikk (1) bekezdés c) pontja nem vonatkozik rá.

A Társaság főtevékenysége vasúti áruszállítás. A Társaság csak korlátozott mennyiségű személyes adatot kezel és kizárólag a főtevékenységével összefüggésben. Figyelembe véve ezen tényeket és a fenti kötelező érvényű rendelkezéseket, a Társaság ügyvezetése azon az álláspontón van, hogy a Társaságra nem vonatkoznak a kötelező érvényű rendelkezések, ezért az a döntés született, hogy adatvédelmi tisztviselő nem kerül kinevezésre.

2.5. AZ ADATKEZELŐ TÁJÉKOZTATÁSI KÖTELEZETTSÉGE

Az adatkezelőnek kötelezettsége, hogy az érintettet a személyes adatai kezeléséről, tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazott tájékoztatást nyújtson.

2.5.1. Eljárásrend

A személyes adatok megszerzésének az alábbi két fő módja van, amelyeket a GDPR tartalmaz:

a) személyes adatoknak az érintettől történő gyűjtése (GDPR 13. cikk)
b) a személyes adatoknak nem az érintettől történő megszerzése (GDPR 14. cikk)

A GDPR mindkét esetre vonatkozóan felsorolja, hogy milyen információkat kell az érintetteknek megadni. Ezen felül további információk is megadhatók. A Tájékoztató összeállítása során az alábbi kérdéseket kell figyelembe venni:

2.5.1.1 Rendelkezik-e már az érintett az információval?

A GDPR megköveteli az érintettek tájékoztatását a felsorolt információkról, kivéve, ha az érintett már rendelkezik ezekkel az információkkal. Ezért fontos annak megállapítása, hogy az érintett rendelkezik minden olyan információval, amelynek átadását előírják és ez megfelelően igazolható-e.

Amennyiben ez a helyzet áll fenn, az előző tájékoztatást dokumentálni kell és meg kell őrizni a GDPR-nak történő megfelelés bizonyítékaként. A tájékoztatás megtörténtént és igazolhatóságát minden érintett esetében egyedileg kell vizsgálni.

2.5.1.2 Amennyiben a személyes adat közvetlenül az érintettől kerül felvételre

Abban az esetben, ha az érintett nem rendelkezik a szükséges információkkal (például amikor az adatgyűjtés a weboldalon történik közvetlenül a felhasználóktól vagy az alkalmazottaktól), a személyes adatok felvételekor az alábbiakról kell tájékoztatást adni:

- az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei;
- az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
- a személyes adatok kezelésének célja, valamint az adatkezelés jogalapja;
- az adatkezelő vagy harmadik fél jogos érdekei;
- az adatkezelés módja;
- adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
- adott esetben annak ténye és részletei, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat,
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- az érintett azon jogairól szóló tájékoztatás, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését, továbbá az érintett adathordozhatósághoz való joga
- az érintett azon jogairól szóló tájékoztatás, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- az érintett azon jogáról szóló tájékoztatás, hogy jogosult a hozzájárulásának bármely időpontban történő visszavonására;
- az érintett azon jogáról szóló tájékoztatás, hogy jogosult felügyeleti hatósághoz címzett panasz benyújtására;
- arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul és hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;
- arról, hogy történik-e automatizált döntéshozatal, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról.

2.5.1.3 *Amennyiben a személyes adat nem az érintettől kerül felvételre*

Ha a személyes adatokat nem az érintettől szerezték meg (például amikor a személyes adatokat egy harmadik fél bocsájtja a Társaság rendelkezésére), számos egyéb körülmény van (azaz azon esetet nem számítva, amikor az érintett már rendelkezik az információval) amikor nem kell információt adni. Ezek az alábbiak:

- a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne,

- az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik; (GDPR 14. cikk)
- a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján, bizalmasnak kell maradnia.

Ahol a feltételek bármelyike alkalmazható, ennek okát megfelelően dokumentálni kell és meg kell őrizni a GDPR megfelelés bizonyítékaként. Ügyelni kell arra, hogy biztosítsák ennek alkalmazását az összes szükséges információra és az összes érintettre.

Amennyiben a fenti feltételek egyike sem áll fent tájékoztatni kell az érintetteket:

- a személyes adatok megszerzésétől számított ésszerű határidőn, de legkésőbb egy hónapon belül;
- ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, (például email címek) legalább az érintettel való első kapcsolatfelvétel alkalmával;
- ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

Az alábbi információkról kell tájékoztatást adni:

- az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei; - az adatvédelmi tisztviselő 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 és részletei, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat,
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- az érintett azon jogairól szóló tájékoztatás, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését, továbbá az érintett adathordozhatósághoz való joga
- az érintett azon jogairól szóló tájékoztatás, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- az érintett azon jogáról szóló tájékoztatás, hogy jogosult a hozzájárulásának bármely időpontban történő visszavonására;

- az érintett azon jogáról szóló tájékoztatás, hogy jogosult felügyeleti hatósághoz címzett panasz benyújtására;
- a személyes adatok forrásáról;
- arról, hogy történik-e automatizált döntéshozatal, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról.

2.5.2 Az érintett tájékoztatása

Mint minden érintettek részére a GDPR-ral összefüggésben szolgáltatott információ, ezt is érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell nyújtani. A tájékoztatás érintettekre részére történő megküldésének legjobb módja az üzleti folyamat sajátosságaitól függ, és az alábbiakat foglalhatja magába:

- Értesítés weboldalon
- E-mail útján
- Nyomtatott levél/tájékoztató útján
- telefonon

Amennyiben a személyes adatok utóbb más célra kerülnek felhasználására, mint amire az adatokat felvételre kerültek, az eltérő célra történő adatkezelés megkezdése előtt az érintettnek szóló tájékoztatást az új tartalom szerint ismét meg kell adni.

A tájékoztatás megtörténtét megfelelően dokumentálni kell, hogy bizonyítható legyen. Eszerint (i) amennyiben a tájékoztatás a weboldalon történt meg kell róla győződni, hogy az érintett hozzáfér a teljes tájékoztatóhoz és aktív magatartással elfogadja azt (kipipál egy négyzetet vagy megnyomja az elfogadás gombot stb.), (ii) ha emailben történik, az e-mail átvételét igazolni kell, (iii) ha levélben történik, az átvételét igazolni kell, ha (iv) személyes átadással történik, az átvételi igazolni kell, továbbá (v) továbbá a telefonhívást megfelelően rögzíteni kell.

A szervezeten belül a tájékoztatók tartalmának jóváhagyására kijelölt személy a Vezérigazgató.

2.6. ÉRINTETTEKTŐL ÉRKEZŐ MEGKERESÉSEK KEZELÉSE

A GDPR az érintettek számára széles jogokat biztosít a saját adataik felett és fontos, hogy a szervezet készen álljon arra, hogy biztosítsa ezeket a jogokat, és határidőben teljesítse a kérelmeket.

2.6.1 Általános szabályok

Minden egyes, érintettől érkező megkeresésre az alábbi általános szabályok irányadók:

- Minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell nyújtani az érintettek részére, különösen a gyermekeknek címzett bármely információ esetében;
- Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni;
- Az érintett kérésére szóbeli tájékoztatás is adható (pl.: telefonon vagy személyesen), feltéve, hogy az érintett személyazonossága megfelelően igazolásra került;
- Az érintettek jogai gyakorlására irányuló kérelmének a teljesítését nem tagadhatjuk meg, kivéve, ha bizonyítjuk, hogy az érintettet nem áll módunkban azonosítani;
- Indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül kell tájékoztatnunk az érintetteket a kérelmek nyomán hozott intézkedésekről; Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatnunk kell az érintetteket;
- Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri;
- Ha nem teszünk intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatnunk kell az érintetteket az intézkedés elmaradásának okairól, valamint arról, hogy az érintettek panaszt nyújthatnak be valamely felügyeleti hatóságnál, és élhetnek bírósági jogorvoslati jogával;
- A tájékoztatást és intézkedést díjmentesen kell biztosítanunk, kivéve, ha egy érintett kérelme „egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó” (GDPR 12. cikk). Ezekben az esetekben a költségekre adminisztratív díjat számítunk fel, vagy megtagadjuk a kérelem alapján történő intézkedést; Az adminisztratív díj kiszámítása az alábbiak szerint történik:
    a) amennyiben a kérelem teljesítéséhez nem szükséges adathordozó rendelkezésre bocsátása, vagy papír alapú dokumentáció fénymásolása, úgy a díj: 3000 Ft/óra.
    b) amennyiben adathordozón kerül átadásra a vonatkozó adat, úgy az adathordozó díja + a) pont szerinti díj
    c) amennyiben papír alapú fénymásolás szükséges, úgy oldalanként további 100 Ft/oldal kerül felszámolásra.
- Ha megalapozott kétségeink vannak a természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérhetjük.

2.6.2 Az eljárás lépései

Lépés	**Leírás**	**Felelős**
Az érintett kérelmének beérkezése	Az érintett a kérelmét elektronikusan (e-mailben vagy a honlapunkon keresztül), postai vagy telefonos úton is előterjesztheti. Ezt a szervezet bármely része befogadhatja, de az ideális az lenne, ha az ügyfélszolgálaton keresztül érkeznének be.	Kérelmet átvevő/érkeztető ügyintéző
Az érintettek kérelmeinek naplózása	A kérelem átvételének tényét és ennek időpontját be kell jegyezni az *Érintettek Kérelmeinek Nyilvántartásá*ba (4. melléklet). A kérelmet benyújtó személy azonosító adatait (név, cím, más azonosító adatok), a kérelem típusát (törlés, javítás, adatok módosítása stb.), az érintett adatokat és a kérés okait is azonosítjuk és rögzítjük a nyilvántartásban. Amennyiben a kérelem nem világos, úgy ezt az érintett részére haladéktalanul jelezni kell, tájékoztatást adva egyben arról, hogy milyen tárgyú kérelmet terjeszthet elő az érintett.	Kérelem Ügyintéző
Az érintett személyazonosságának igazolása	Az érintett személyazonosságának igazolására a kérelem előterjesztésének módjától függő belső eljárásrend szerinti módszerrel kerül sor. Amennyiben szükséges további információ kérhető a személyazonosság igazolásához. Ha az érintett a személyazonosságát nem tudja igazolni, a kérelmet elutasítjuk, és ennek okát haladéktalanul, de legkésőbb az ilyen kérelem kézhezvételétől számított egy hónapon belül közöljük az érintettel.	Kérelem Ügyintéző

A kérelem érvényességének értékelése	Alkalmazni kell annak megállapítására irányuló tesztet, hogy a kérelem „egyértelműen megalapozatlan vagy túlzó”. Ezt az Érintettek Kérelmeinek Nyilvántartása ellenőrzésével kell végrehajtani, hogy benyújtott-e kérelmező már korábban is hasonló kérelmet, valamint értékelni kell a kérelem típusát. Ha igen, akkor dönteni kell arról, hogy visszautasítjuk a kérelmet vagy külön költségtérítés ellenében teljesítjük. Helyesbítésre, törlésre, az adatkezelés korlátozására és adatkezelés elleni tiltakozásra irányuló kérelem esetében dönteni kell arról, hogy a kérelem ésszerű és jogszerű-e. Ha nem, akkor a kérelmet vissza kell utasítani és a késedelem nélkül, de legfeljebb a kérelem beérkezésétől számított egy hónapon belül tájékoztatnunk kell az érintettet a döntésről, valamint arról, hogy az érintett panaszt nyújthat be a felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.	Kérelem Ügyintéző
Lépés	**Leírás**	**Felelős**
Díj kiszabása	Amennyiben díjfizetés kiszabására kerül sor, az érintettet tájékoztatni kell ennek tényéről és biztosítani kell számára a döntés lehetőség, hogy folytatja-e az eljárást vagy sem. Amennyiben az érintett úgy dönt, hogy nem folytatja az eljárást, a kérelmet vissza kell utasítani és ennek okát haladéktalanul közölni kell.	Kérelem Ügyintéző
A kért információk összeállítása	Amennyiben a kérelem megalapozott és teljesíthető, úgy a kérelem típusának megfelelően össze kell gyűjteni a releváns információkat. Ez magában foglalja annak megtervezését is, hogy a kérelmezett műveletet (pl.: az adatkezelés korlátozása vagy törlése) hogyan lehet elvégezni A kérelmet legfeljebb 1 hónapon belül teljesíteni kell, mely határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatni kell az érintettet.	Kérelem Ügyintéző / Adattulajdonos

Tegye meg a kért műveletet / adja meg a kért információkat	A kérelmezett műveletet el kell végezni (amennyiben lehetséges) és a kérelmezett tájékoztatást meg kell küldeni az érintett részére elektronikus úton, ha azt választotta, vagy írásban, postai úton.	Kérelem Ügyintéző
Az érintett kérelmének lezárása	A kérelem megválaszolásának tényét és ennek módját (teljesítés/visszautasítás) a kérelem lezárásnak időpontjával naplózni kell az *Érintettek Kérelmeinek Nyilvántartásá*ban.	Kérelem ügyintéző

A jelen Adatvélelmi Szabáályzat 4. számú mellékletét képezi az Érintettek Kérelmeinek Nyilvántartásaként használandó táblázat.

2.6.3 Az érintett lehetséges kérelmei

2.6.3.1 A hozzájárulás visszavonásához való jog

Amennyiben az adatkezelés jogalapját az érintett hozzájárulása képezi (és nincs más jogalap, mint például a szerződéses vagy jogi kötelezettség teljesítése), az érintett jogosult a hozzájárulását visszavonni.

Az érintett személyes adatainak adatkezelésből történő törlését megelőzően meg kell erősíteni azt, hogy valóban a hozzájárulás-e az adatkezelés jogalapja. Ha nem, a kérelmet vissza lehet utasítani azzal az indoklással, hogy az adatkezelés más jogalapon történik és nem szükséges az érintett hozzájárulása. Ellenkező esetben a kérelmet teljesíteni kell. A kérelmet minden esetben részletesen ki kell értékelni, és a lehető legteljesebb mértékben kell teljesíteni, és minden elutasítást (részleges elutasítást is) indokolni kell.

Az Adatkezelőnek biztosítania kell azt, hogy az érintett a hozzájárulását bármikor visszavonhassa, és a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tennie, mint annak megadását.

A legtöbb esetben a hozzájárulás megadására és visszavonására elektronikus úton, azaz online lehetőség van (pl. profil törlése) így erre az eljárásra nem lesz szükség.

Amennyiben gyermek beleegyezésére van szükség (16 éves kor alatti személyek), a hozzájárulás megadását vagy visszavonását annak a személynek kell jóváhagynia, aki a gyermek szülői felügyeleti jogát gyakorolja, továbbá ezen személy(ek) személyazonosságát szintén meg kell vizsgálni és rögzíteni kell az Érintettek Kérelmeinek Nyilvántartásában a ‘Megjegyzések’ között.

2.6.3.2 *A tájékoztatáshoz való jog*

Az érintettek részére a személyes adatok megszerzésének időpontjában tájékoztatást kell adni a személyes adatok kezelésének tényéről, céljáról, jogalapjáról, a kezelt adatok köréről, az adatkezelés módjáról, időtartamáról vagy az időtartam meghatározásának szempontjairól, az adattovábbítás szabályairól, a felügyeleti hatósághoz címzett panasz benyújtásának jogáról.

A tájékoztatás mellett az érintett figyelmét kifejezetten fel kell hívni a tiltakozáshoz való jog érvényesítésének lehetőségére, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

A tájékoztatást:

a) az álláspályázatot benyújtók számára az álláspályázati felhívás közzétételét szolgáló oldalon a vonatkozó adatkezelési tájékoztató szerinti tartalommal kell nyújtani;
b) az Adatkezelővel munkaviszonyt, munkavégzésre irányuló egyéb jogviszonyt létesítő személyek részére a jogviszony létrejöttekor a vonatkozó adatkezelési tájékoztatók szerinti tartalommal kell nyújtani;
c) az Adatkezelő területére belépő személyek részére a területre való belépés előtt a vonatkozó adatkezelési tájékoztatók szerinti tartalommal kell nyújtani.

Az a) pont szerinti tájékoztatást az Adatkezelő honlapján, tömör, átlátható, és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell elhelyezni.
A b) pont szerinti tájékoztatást a jogviszony létesítésekor elektronikus formában kell megadni, melynek megtörténtét az érintett papír alapú nyilatkozatával írásban igazolni köteles.
A c) pont szerinti tájékoztatást a területhatáron lévő kerítés vagy beléptető kapura való kiragasztással, kitáblázással kell elhelyezni.

2.6.3.3 *Az érintett hozzáférési joga*

Az érintettek jogosultak arra, hogy visszajelzést kapjanak tőlünk arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosultak arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjanak:

- az adatkezelés céljai;
- az érintett személyes adatok kategóriái;
- azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közöltük vagy közölni fogjuk, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
- a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

- az érintett azon joga, hogy kérelmezheti tőlünk 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;
- automatizált döntéshozatal ténye, ideértve a profilalkotást is, és arra vonatkozó információk, hogy ez 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 garanciákról.

A személyes adatokhoz való hozzáférést úgy kell biztosítani, hogy ez alatt az érintett más személy személyes adatait lehetőleg ne ismerhesse meg. Ez alól kivételt képezhetnek azok a személyes adatok, amelyek mind az érintettre, mind pedig egy másik személyre vonatkoznak.
Az érintett hozzáféréshez való jogát az Adatkezelő az elérni kívánt céllal arányosan korlátozhatja vagy megtagadhatja, ha ezen intézkedés elengedhetetlenül szükséges:

a) az Adatkezelő részvételével végzett vizsgálatok vagy eljárások – így különösen büntetőeljárás – hatékony és eredményes lefolytatásának;
b) bűncselekmények hatékony és eredményes megelőzésének és felderítésének;
c) bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtásának;
d) a közbiztonság hatékony és eredményes védelmének;
e) az állam külső és belső biztonsága hatékony és eredményes védelmének, így különösen honvédelem és nemzetbiztonság; vagy
f) harmadik személyek alapvető jogai védelmének biztosításához.

Amennyiben az Adatkezelő megtagadja vagy korlátozza az érintett hozzáférési jogát, erről haladéktalanul írásban tájékoztatja érintettet – amennyiben a korlátozás, megtagadás célját ez nem veszélyezteti – az intézkedés indokát is megjelölve. A tájékoztatásban az Adatkezelő külön felhívja érintett figyelmét, hogy hozzáférési jogát a felügyeleti hatóság közreműködésével is gyakorolhatja. Abban az esetben, ha a kezelt adat tárolása vagy mentése hang vagy videó-felvétel formájában történt, az anyagot eredeti formában kell kiadni, jegyzőkönyvek vagy kivonatok csak akkor elegendők, ha az eredeti felvételek már megsemmisültek.

2.6.3.4 A helyesbítéshez való jog

Az érintett kérelmére az adatkezelést végző illetékes ügyintéző indokolatlan késedelem nélkül helyesbíti az érintettre 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 is.
Szükség esetén a Társaság intézkedések tesz az érintettektől érkező információ ellenőrzése érdekében, hogy biztosítsa a pontosságukat még azok rögzítése előtt (pl. személyes okmányokba történő betekintés útján).

2.6.3.5 *A törléshez való jog („az elfeledtetéshez való jog")*

Az érintett kérelmére az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő indokolatlan késedelem nélkül törli az érintett személyes adatait vagy azoknak az érintett által meghatározott körét, feltéve, hogy az alábbi esetek valamelyike fennáll:

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett a GDPR 21. cikk (1) bekezdése alapján tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a GDPR 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;
- a személyes adatokat jogellenesen kezelték;
- a személyes adatokat uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

Ésszerű erőfeszítéseket kell tenni a törlés biztosítása érdekében abban az esetben, ha az adatok nyilvánosságra kerültek. Ez azt jelenti, hogy figyelembe véve rendelkezésre álló technológiát és alkalmazásának költségeit a Társaság köteles minden ésszerű intézkedést megtenni, annak érdekében, hogy tájékoztassa a személyes adatok adat kezelőjét arról, hogy az érintett kérelmezte az adatkezelőtől az ilyen személyes adataira mutató hivatkozások, valamint a személyes adat másolatainak és replikációinak törlését.

Az Adatkezelő a személyes adatok törlését a jogszerű kérelem ellenére sem végezheti el, amennyiben az adatkezelés szükséges:

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
- jogszabályban előírt kötelezettségnek való megfelelés céljából;
- népegészségügy területét érintő közérdek alapján;
- a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból; - jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

Valószínű, hogy ezen döntések meghozatalába szükséges lesz bevonni a Társaság Adatvédelmi Tisztviselőjét, ha van ilyen, illetve bizonyos esetben a Társaság felső vezetését.

2.6.3.6 Az adatkezelés korlátozásához való jog

Az érintett kérelmére az adatkezelést végző illetékes ügyintéző 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 ellenőrizzük 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;
- 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.

Az adatkezelést korlátozó érintettet a korlátozás feloldása előtt arról tájékoztatnia kell.

A Társaságnak minden egyes ilyen kérelem esetében döntenie kell arról, hogy a kérelem engedélyezhető-e. Valószínű, hogy ezen döntések meghozatalába szükséges lesz bevonni a Társaság Adatvédelmi Tisztviselőjét, ha van ilyen, illetve bizonyos esetben a Társaság felső vezetését.

Ha az adatkezelés a fentiek szerint 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.
(3) Az adatkezelést végző illetékes ügyintéző az érintettet, akinek a kérésére az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

A címzettek és adatfeldolgozók tájékoztatásának kötelezettsége

Az Adatkezelő minden olyan címzettet és adatfeldolgozót tájékoztat a személyes adatot érintő valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölte, illetve akinek továbbította, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

2.6.3.7 *Az adathordozhatósághoz való jog*
Az érintett kérelmére az adatkezelést végző illetékes ügyintéző biztosítja a személyes adatok hordozhatóságát az alábbi feltételek teljesülése esetén:

a) a személyes adatokat az érintett bocsátotta az Adatkezelő rendelkezésére;
b) az adatkezelés jogalapja hozzájárulás vagy az érintett és az Adatkezelő között kötött szerződés;
c) adatkezelés automatizált módon történik;
d) a személyes adatok hordozása nem érinti hátrányosan mások jogait vagy szabadságait.

Az adathordozhatósághoz való jog gyakorlása során az Adatkezelő köteles a személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban az érintett rendelkezésére bocsátani (PDF/XML).

Az érintett kérheti, hogy az Adatkezelő a személyes adatokat közvetlenül egy másik adatkezelő részére továbbítsa. E lehetőséggel az érintett abban az esetben élhet csak, ha az technikailag megvalósítható.

Az Adatkezelő emellett – a hozzáféréshez való jog érvényesülésének elősegítése érdekében – papír alapon is köteles rendelkezésre bocsátani a személyes adatokat.
Az e kategória alá tartozó szolgáltatások esetében minden egyes ügy esetében minimális döntéshozatali eljárás szükséges, és nagyon kívánatos, hogy ezen folyamat végrehajtása automatizált legyen.

2.6.3.8 A tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak alábbi jogi indokokon alapuló kezelése ellen:

- 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.

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.

Ha a személyes adatok kezelésére a GDPR 89. cikk (1) bekezdése alapján 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.

Ha tiltakozást nyújtottak be a Társaságnak igazolnia kell az okokat, amire az adatkezelést alapítják és ennek megtörténtéig fel kell függeszteni az adatkezelést. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik (ideértve a profilalkotást), nincs más választásunk csak az, hogy az adatkezelést beszüntetjük.

Tiltakozás esetén az Adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha 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.

2.6.3.9 *Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást*

Az 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 és szükség esetén ragaszkodhat az emberi beavatkozáshoz. Az érintettnek jogában áll kifejteni álláspontját és a döntéseket vitatni.

Ezen jog alól vannak bizonyos kivételek, amelyek akkor állnak fent, ha a döntés:

- szerződés megkötése vagy teljesítése érdekében szükséges;
- jogszabály lehetővé teszi;
- az érintett kifejezett hozzájárulásán alapul.

Az ilyen típusú kérelmek megítélésekor meg kell határozni, hogy a fenti kivételek a szóban forgó konkrét esetben alkalmazhatók-e.

2.6.3.10. Jogorvoslathoz való jog

Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett az adatkezelő ügyfélszolgálatához ***adatvedelem@ewgrail.com*** fordulhat, aki a panaszt megvizsgálja, és ha alapos, az Adatkezelő vezérigazgatójához intézkedést kezdeményez, ellenkező esetben a panaszt elutasítja.

Az elutasításról az Adatkezelő a panaszost a kérelem kézhezvételét követő 30 napon belül írásban tájékoztatja, a kérelem elutasításának ténybeli és jogi indokait is közölve. A kérelem elutasítása esetén a panaszost tájékoztatni kell a bírósági jogorvoslat, továbbá a felügyeleti szervhez fordulás lehetőségéről is. Az elutasított kérelmekről az adatkezelő ügyintézője jegyzőkönyvet köteles felvenni.

Ha az érintett továbbra is sérelmezi azt, ahogy az Adatkezelő kezeli az adatait, vagy közvetlenül hatósághoz szeretne fordulni, akkor bejelentéssel élhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (cím: 1055 Budapest, Falk Miksa utca 9-11., postacím: 1363 Budapest, Pf.: 9. E-mail: ugyfelszolgalat@naih.hu, honlap: www.naih.hu).

Az érintettnek lehetősége van továbbá személyes adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el. Ebben az esetben az érintett szabadon választhat, hogy a lakóhelye (állandó lakcím) vagy a tartózkodási helye (ideiglenes lakcím) szerinti törvényszéknél (http://birosag.hu/torvenyszekek) nyújtja-e be keresetét.
Az érintett a lakóhelye vagy tartózkodási helye szerinti törvényszéket megkeresheti a http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso oldalon.

2.7. IRATKEZELÉSI ÉS SELEJTEZÉSI SZABÁLYOK

A Társaságnál hatályban lévő iratkezelési és selejtezési szabályokat a mindenkor hatályos Iratkezelési és selejtezési Szabályzat tartalmazza.

2.8. AZ ADATBIZTONSÁG KÖVETELMÉNYE

Az Adatkezelő 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 biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik. Ideértve többek között, adott esetben:

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

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.

Az Adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt a jelen Szabályzatban foglalt elvek hatékony megvalósítása, másrészt a további adatvédelmi garanciák beépítése az adatkezelés folyamatába.

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

Személyes adatot tartalmazó irat nem hagyható olyan helyen, ahol harmadik személy is hozzáférhet. Az ilyen iratok elzárásáról azokban az irodákban, illetve személyzeti helyiségekben is gondoskodni kell, ahol az illetékes iratkezelőkön kívül más, harmadik személy is megfordulhat.

A manuálisan kezelt személyes adatok elvesztésének megelőzése érdekében eredeti iratokat csak hivatalos ügyintézés, különösen bírósági eljárás vagy nyomozati eljárás során lehet kiadni. Kiadást megelőzően az eredeti iratokról az illetékes szervezeti egységnél történő megőrzés céljára hiánytalan másolatot kell készíteni.

Személyes adatokat ért sérülés vagy megsemmisülés esetén a rendelkezésre álló egyéb adatforrásokból meg kell kísérelni a lehetséges mértékig a károsodott adatok pótlását. A sérült adat pótlására annak a szervezeti egységnek a vezetője felelős, ahol a sérülés bekövetkezett. Az adatpótlásba be kell vonni azon illetékes adatkezelő személyt, aki az adatok rögzítésében közreműködött. A pótolt adatokon a pótlás tényét fel kell tüntetni.

A Társaság által kezelt személyes adatokat a Társaság elektronikus formában és/vagy papír alapon is tárolja.

Az adatok biztonsága érdekében a Társaság megfelelő szervezeti és technikai intézkedéseket alkalmaz. A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe vesszük 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.

Az elektronikus formában tárolt adatok saját szerveren kerülnek tárolásra a Társaság székhelyén, illetve fióktelephelyén.

Az elektronikus levelezés O365 rendszerrel, a Microsoft, mint adatfeldolgozó által nyújtott szolgáltatásként kerül tárolásra.

Lokális hardverekre történő mentéseket az IT szabályzat tartalmazza.

Az elektronikusan tárolt adatok biztonsága érdekében alkalmazott további szervezeti és IT biztonsági intézkedéseket az IT Szabályzat tartalmazza.

A személyes adatokat tartalmazó papír alapú dokumentumok külön irattári szabályok szerint kerülnek lefűzésre. A személyes adatokat tartalmazó mappákat zárható szekrényben tároljuk a Társaság székhelyén, melyet minden nap nyitunk és zárunk. A szekrény kulcsai zárható páncélszekrényben vannak elhelyezve. Az iratszekrények hozzáférése külön utasítások szerint üzleti részlegenként kerül meghatározásra.

Az fióktelepre való belépések körében alkalmazott biztonsági intézkedéseket a Létesítményvédelmi Szabályzat tartalmazza.

Az adatbiztonság követelményének érvényesüléséről az Adatkezelő a jelen Szabályzattal, illetve külön utasításokkal, szabályzatokkal gondoskodik. Az Adatkezelő gondoskodik arról, hogy a jelen Szabályzat, valamint a külön utasítások és szabályzatok mindenkor hatályos tartalmát a munkavállalói, illetve érdekkörében eljáró harmadik személyek (így különösen az adatfeldolgozók) megismerjék, és ezeknek megfelelően járjanak el.

2.9. AZ ADATKEZELÉS SPECIÁLIS ESETEI

2.9.1. A munkavállalók adatainak kezelése

Az Adatkezelő valamennyi munkaviszonyt vagy munkavégzésre irányuló egyéb jogviszonyt létesítőt köteles tájékoztatni a munkavégzéssel kapcsolatos adatkezelésekről. A tájékoztatás megismeréséről az érintett írásban nyilatkozik.

A bér- és munkaügyi nyilvántartás adatai a foglalkoztatott jogviszonyával kapcsolatos tények megállapítására, a besorolási követelmények igazolására, bérszámfejtésre, társadalombiztosítási ügyintézésre és statisztikai adatszolgáltatásra használhatók fel.

A bér- és munkaügyi nyilvántartás kezelését – a feladatkörük ellátásához szükséges mértékben – az Adatkezelő személyzeti ügyekért felelős munkavállalója végzi.

2.9.2. Manuálisan kezelt személyes adatok

Az Adatkezelőnek az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül

azt kell választania, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene a Társaságnak.

A manuálisan kezelt személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani:

a) az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni;
b) a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá, a személyzeti, a bér- és munkaügyi iratokat biztonságosan elzárva kell tartani,
c) az adatkezelések iratainak archiválását rendszeresen el kell végezni, az archivált iratokat a vonatkozó előírásoknak megfelelően kell szétválogatni és irattári kezelésbe venni.

A b) pont szerinti helyiségek, illetve szekrények kulcsához való hozzáférés rendjét az Adatkezelő vezérigazgatója állapítja meg.

2.9.3. Elektronikusan kezelt személyes adatok

Amennyiben az Adatkezelő olyan elektronikus rendszerben kezel személyes adatot, amelybe csak a hozzáférési listára felvett, nyilvántartott, illetékes munkavállaló léphet be, úgy az illetékes munkatársnak egyéni, titkos jelszóval kell bejelentkeznie a rendszerbe. Az adatkezelés befejeztével a rendszerből ki kell lépni. A rendszerben történt, jelszóval védett adatkezelésért az Adatkezelő felel.

Az adatvédelmi incidensek elkerülése érdekében a munkavállaló kötelessége az egyéni jelszavának védelme. Az egyéni jelszó a munkavállalón kívül kizárólag az adatkezelési szoftver fejlesztését, üzemeltetését ellátó informatikai munkatársak, valamint a Vezérigazgató által ismerhető meg, ha az az Adatkezelőnél elvégzendő feladatuk ellátásához szükségessé válik.

Az adatkezelésre használt számítógépek adatbevitelre, lekérdezésre alkalmas állapotban történő, felügyelet nélkül hagyása tilos.

Az Adatkezelő kizárólag olyan adatkezelési rendszert alkalmazhat, amely a rendszerbe történt belépést regisztrálja, illetve a rögzített adatokról megállapítható, hogy az adatrögzítés ki által és milyen időpontban történt.

2.9.4. A munkavállalókat érintő ellenőrzések szabályai

<u>2.9.4.1. Postai küldemények</u>

A munkahelyre érkezett postai küldemény, amennyiben feltételezhető, hogy az személyre szóló – például „s.k.” jelzéssel lett ellátva, vagy a címzett pontos nevét feltüntették – először a munkavállalónak

kell átadni. Amennyiben ilyen tartalmú levél mégis felbontásra kerül, akkor azt vissza kell zárni, és a felbontás dátumát, valamint a levél tartalmának megismerő személy nevét fel kell rajta tüntetni.

2.9.4.2. Telefonok használatának ellenőrzése

Az Adatkezelő által a munkavállalók rendelkezésére bocsátott mobil és vezetékes telefonokat elsődlegesen hivatalos célból lehet használni, a magáncélú használat alkalomszerűen, az erőforrások arányos igénybevételéig engedélyezett.

Amennyiben az Adatkezelő, mint munkáltató a jogos érdekére hivatkozva ellenőrizni kívánja a munkavállalók telefonhasználatát, akkor ez kizárólag a hivatalos használatra terjedhet ki, a magáncélú használat ellenőrzése tilos. Az ellenőrzés során főszabály szerint az Adatkezelő biztosítja a munkavállaló jelenlétét és ellenőrzés során a fokozatosság elvének betartásával jár el. Az ellenőrzés lefolytatása előtt a munkáltatói jogkörgyakorló köteles a munkavállalót az adatkezelés körülményeiről tájékoztatni. Amennyiben a munkáltatói ellenőrzés a munkavállalóhoz köthető híváslista ellenőrzéséhez kapcsolódik, akkor a távközlési szolgáltatótól meg kell kérni az adott telefonszámhoz tartozó részletes híváslistát olyan módon, hogy a híváslistában szereplő telefonszámok utolsó három számjegye nem felismerhető formában (anonimizáltan) szerepeljen, amely alapján a munkavállaló a magáncélú hívásait kiválogathatja. Ezt az anonimizált híváslistát kizárólag az érintett munkavállaló és a munkáltatói jogkörgyakorló ismerheti meg.

Abban az esetben, ha a munkavállaló visszaadja az általa használt mobiltelefont akár a munkaviszony fennállása alatt, akár a munkaviszony megszűnésekor, gondoskodni kell arról, hogy az eszközön tárolt esetleges magánjellegű adatokat – így telefonszámokat, üzeneteket, képeket, filmeket, egyéb formájú és tartalmú adatokat – az érintett lementhesse, majd azokat visszaállíthatatlan módon törölni kell. A munkavállaló köteles a magánjellegű tartalmak eltávolításáról jelen Szabályzat 7. számú mellékletében foglaltak szerinti formában és tartalommal írásbeli nyilatkozatot tenni. A készüléket csak azt követően lehet átadni harmadik személy részére, ha az eszközkiadásért felelős személy meggyőződött arról, hogy azon magánjellegű adat már nincs, vagy nem fellelhető. Az eljárást lefolytató személyt a megismert magánjellegű adatok tekintetében titoktartási kötelezettség terheli, azt harmadik személy részére nem adhatja át, rá vonatkozó információt nem közölhet.

2.9.4.3. E-mail postafiók használatának és ellenőrzésének adatvédelmi szabályai

Az Adatkezelő a munkavégzés céljára rendelkezésre bocsátott e-mail postafiókot hivatalos célból adja át a munkavállalónak, mely fiók magáncélra nem használható.

Az Adatkezelő informatikai rendszereinek üzembiztos működéséért felelős szervezeti egysége (IT) jogosult az e-mail postafiók tárolókapacitását meghatározni, az e-mailhez csatolt fájlok méretét és formátumát korlátozni, és köteles az ezzel kapcsolatos információkról a munkavállalókat szükség

szerint, de legalább fél évente e-mailben tájékoztatni. E beállításokat, és a szervezeti egység által meghatározott további felhasználói szabályokat a munkavállalók kötelesek betartani.

A munkavállaló további nem üzleti e-mail postafiókokat a munkahelyi számítógépen megnyithat, és használhat azzal, hogy az ilyen magáncélú használat során az Adatkezelő üzleti érdekeit és jó hírnevét nem sértheti.

Az Adatkezelő, mint munkáltató jogos érdekére hivatkozva ellenőrizheti a munkavállaló által folytatott hivatalos levelezést a jelen Szabályzatban foglaltak betartásával. Az ellenőrzés során az Adatkezelő fő szabály szerint biztosítja a munkavállaló személyes jelenlétét, továbbá az ellenőrzés során a fokozatosság elvének betartásával jár el. Az ellenőrzés alapját az Adatkezelő által elkészített érdekmérlegelési teszt eredménye adja. Az ellenőrzésre jogosult munkáltatói jogkör gyakorló köteles a munkavállalót dokumentált módon, a tényleges ellenőrzés megkezdése előtt tájékoztatni, hogy mely, pontosan meghatározott érdek miatt kerül sor az ellenőrzésre. A munkavállaló az ellenőrzés során az e-mail tartalmának megtekintése előtt köteles jelezni a munkáltatónak, illetve a munkáltató képviseletében eljáró személynek, ha az adott e-mail személyes adatot tartalmaz. A munkaköri feladatokkal kapcsolatos e-mailek tartalmát az Adatkezelő korlátozás nélkül vizsgálhatja.

Amikor a hivatalos e-mail postafiók tartalmát a munkáltató ellenőrizni kívánja – a lépcsőzetes ellenőrzési rendszer alapján –, elsősorban a levelek fejlécének listáját jogosult az IT szervezeti egységtől megkérni. A lista tartalmazhatja a postafiókba érkezett és onnan küldött levelek címzettjét, tárgyát, valamint, amennyiben további adat ismerete szükséges a küldés vagy fogadás időtartamát, és az esetlegesen csatolt fájl nevét, méretét. A lista megismerését követően a munkáltatói jogkörgyakorló kijelölheti azokat a leveleket, amelyeket a munkavállalónak át kell adnia, aki a kérést csak abban az esetben jogosult megtagadni, ha a levél magánjellegű. A magánjellegű levelek tartalmát a munkáltató nem ismerheti meg. A tilalom ellenére folytatott magánjellegű levelezés esetében ugyanis a levél tartalmának megismerése nem szükséges a munkavállalóval szemben esetlegesen alkalmazandó munkajogi jogkövetkezményekhez. Ilyen levelek törlésére a munkáltatói jogkörgyakorló jogosult felszólítani a munkavállalót, a munkavállaló pedig köteles eleget tenni a felszólításnak.

Amennyiben olyan időpontban kellene az e-mail postafiókban tárolt levelek közül a szükséges hivatalos tárgyú leveleket kiválogatni, amikor az érintett munkavállaló tartósan nem tartózkodik a számítógép mellett, az érintett kijelölhet olyan munkavállalót, aki helyette a postafiókba belépve ezt megteheti. Ennek hiányában a közvetlen vezető jelölhet ki két személyt, akik együttes jelenlétük mellett csak a meghatározott, hivatalos tárgyú leveleket menthetik le a postafiókból, a nem hivatalos tárgyú levelek tekintetében azonban titoktartási kötelezettsége áll fenn, annak tartalmát nem adhatják át, arról információt nem közölhetnek a vezetővel, vagy más személlyel.

Amennyiben a munkavállalót felmentik a munkavégzés alól, a felmentés időtartamára, illetve a munkavégzésre irányuló jogviszonya megszűnésétől számított legfeljebb három hónapos időtartamban

a munkavállaló e-mail címét a munkavállaló és más munkavállalók számára hozzáférhetetlenné kell tenni (zárolni), valamint olyan informatikai beállítást kell életbe léptetni, amely a postafiók címre küldött levél feladóját automatikus válaszban arról tájékoztatja, hogy:

- a postafiók használata megszűnt, és
- amennyiben hivatalos tárgyú levelet kíván az Adatkezelő részére megküldeni, azt mely e-mail vagy postacímre teheti meg.

A fenti határidő leteltét követően az e-mail postafiók címet inaktívvá kell tenni, vagyis olyan informatikai beállítást kell életbe léptetni, amely megakadályozza, hogy a postafiók további levelet fogadhasson.

A fenti tájékoztatásban nem lehet adatot, információt szolgáltatni arról, hogy az e-mail postafiók használata mely okból szűnt meg, illetőleg, hogy az érintett munkavállaló jogviszonya megszűnt-e, ha igen, a megszűnés mely okból történt.

A postafiók hozzáférhetetlenné, illetve inaktívvá tétele mellett tilos olyan beállítás alkalmazása, mely a postafiókba érkező leveleket más e-mail címre továbbítaná.

A munkavállaló számára az utolsó munkában töltött napján – de legkésőbb az attól számított öt munkanapon belül – biztosítani kell, hogy az esetlegesen postafiókjába érkezett magán jellegű leveleit a postafiókjából lementhesse. E mentést csak akkor kontrolálhatja egy erre kijelölt munkavállaló, ha a jogviszony megszűnésének oka azt indokolja. Ebben az esetben a kijelölt munkavállalót titoktartási kötelezettség terheli a tudomására jutott magánjellegű adatok tekintetében.

Ha a postafiók olyan jellegű hivatalos levelezést tartalmaz, amely a későbbi feladatok ellátása tekintetében szükséges lehet, és a dokumentumok lementése az Adatkezelő részére aránytalan nehézséget okoz, akkor a magánjellegű adatok lementését és végleges eltávolítását követően a postafiók tovább működtethető, melyről az érintett munkavállalót is tájékoztatni kell. A postafiókban a továbbiakban csak hivatalos tárgyú levelek kezelhetők.

2.9.4.4. A munkavállalók rendelkezésére bocsátott internethasználatnak és ellenőrzésének adatvédelmi szabályai

A munkavállalók rendelkezésére bocsátott internet kapcsolat célja elsődlegesen a hatékony munkavégzés elősegítése, emellett a szolgáltatás magán célú használata – az Adatkezelő üzleti érdekeinek, jó hírnevének sérelme, valamint az informatikai rendszer kapacitásainak aránytalan korlátozása nélkül – megengedett.

Az Adatkezelő informatikai rendszereinek üzembiztos működéséért felelős szervezeti egysége (IT) jogosult az internet felhasználást korlátozni, és meghatározni azokat a kulcsszavakat, amelyeket tartalmazó weboldalak megnyitását az informatikai rendszer automatikusan elutasít. Ezen szabályokat a vonatkozó belső szabályzat tartalmazza.

Amennyiben megalapozottan vélelmezhető, hogy a munkavállaló az internet kapcsolatot a fenti szabályok megsértésével használja, a munkáltatói jogkörgyakorló a szabályszegés körülményeit fő szabály szerint személyes elbeszélgetés útján köteles tisztázni.

Amennyiben a fenti eljárás nem vezetne eredményre, a munkáltató kérheti az IT szervezet bevonását azzal, hogy az érintett munkavállaló számítógépén megnyitott weboldalak listáját a munkáltató részére adják át. Ebben az esetben az adatkezelés jogalapját a munkáltató jogos érdeke képezi, amely a munkáltató által elvégzett érdekmérlegelési teszten alapul. A munkáltató listát fő szabály szerint az érintett munkavállaló jelenlétében jogosult ellenőrizni, és a nem hivatalos jellegű adatokat csak a szükséges mértékben és ideig kezelheti, azzal, hogy azokat részleteiben nem ismerheti meg, nem kezelheti, pusztán az esetleges munkajogi következmények megállapításához szükséges mértékben jogosult az adatokat észrevételezni.

2.9.4.5. A munkavállaló munkaállomásának ellenőrzése

Azt a területet, ahol a munkavállaló dolgozik – így például az íróasztalának fiókját – munkaügyi célból nem lehet ellenőrizni. Amennyiben egyéb célból az ellenőrzés szükségessége felmerül, úgy azt csak abban az esetben lehet megtenni, ha a vonatkozó jogszabályi rendelkezések azt lehetővé teszik, és ezt az adatvédelmi tisztviselő előzőleg jóváhagyta. A munkavállalót minden esetben teljeskörűn tájékoztatni kell előzetesen az ellenőrzéssel kapcsolatban megvalósuló adatkezelésről.

2.10. ELSZÁMOLTATHATÓSÁG

2.10.1. Az adatkezelésre és az adatfeldolgozásra vonatkozó általános követelmények.

Az Adatkezelővel jogviszonyban álló személy (személyi hatály), aki személyes adat birtokába jut, ilyet munkaköre vagy tisztsége alapján kezel, köteles védeni és őrizni a személyes adatokat, és minden erőfeszítést megtenni annak érdekében, hogy azoknak megfelelő védelmét biztosítsa.

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

Az Adatkezelővel jogviszonyban állók, illetve az Adatkezelő képviseletében eljáró személyek kötelesek bizalmasan kezelni minden olyan személyes adatot, amely számukra a jogviszonyukkal összefüggésben vált ismertté.

Az Adatkezelővel jogviszonyban álló, adatkezelést vagy adatfeldolgozást végző személyek felelősséggel tartoznak minden olyan kárért, amely adatkezelési, adatvédelmi kötelezettségük megszegéséből származik.

Ha az adatkezelést az Adatkezelő nevében más végzi, az Adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés követelményeinek való megfelelést és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.
Az adatfeldolgozó által végzett adatkezelést olyan szerződésnek kell szabályoznia, amely köti az adatfeldolgozót az Adatkezelővel szemben. A szerződés kizárólag írásban köthető meg.
A szerződésben rögzíteni kell különösen az alábbiakat:

a) az Adatkezelő és az adatfeldolgozó megnevezése;
b) az adatkezelés tárgya;
c) a kezelendő személyes adatok típusa;
d) a kezelendő személyes adatok mennyisége (ha lehetséges);
e) az érintettek kategóriái;
f) az adatkezelés jellege és célja;
g) az adatkezelés jogalapja;
h) az adatkezelés időtartama;
i) teendők az adatkezelési szolgáltatás nyújtásának befejezés esetén;
j) az Adatkezelő kötelezettségeit és jogai;
k) 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;
l) az Adatkezelő és az adatfeldolgozó közötti utasításadás, illetve kapcsolattartás módja;
m) a további adatfeldolgozó igénybevételére vonatkozó döntés;
n) az adatfeldolgozó a további adatfeldolgozó igénybevételére vonatkozóan tiszteletben tartja a jogszabályi előírásokat;
o) titoktartási kötelezettség;
p) adatbiztonsági előírások;
q) közreműködés az adatbiztonsági előírások érvényesítésében, az incidensek kezelésében és a hatásvizsgálatok elvégzésénél;
r) közreműködés az érintetti jogok gyakorlásában;
s) információk nyújtása az Adatkezelőnek és az Adatkezelő ellenőrzési jogosultsága;
t) az Adatkezelő ellenőrzésének kivitelezési módja;
u) a felelősség egyes kérdései;
v) a jogérvényesítési lehetőségek.

Amennyiben szükséges, az adatkezelő és az adatfeldolgozó további intézkedéseket hoz annak biztosítására, hogy az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat.

2.10.2. Az adattovábbításra vonatkozó követelmények

Az Adatkezelő szervezeti rendszerén belül a személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – olyan szervezeti egységhez, személyhez továbbíthatók, amelynek az Adatkezelőnél végzett feladatának ellátásához a személyes adatok megismerése és kezelése szükséges.

Az Adatkezelőnél különböző célra irányuló adatkezelések csak törvényes céloknak megfelelően, indokolt esetben kapcsolhatók össze.

Olyan megkeresés, amely az Adatkezelő által kezelt személyes adat továbbítására irányul csak jogszabályi előírás alapján, vagy csak az alábbi bekezdésben foglalt feltételek fennállása esetén teljesíthető. Minden más esetben az adattovábbítás teljesítését meg kell tagadni.

Olyan esetben, amikor az adattovábbítás nem jogszabályi kötelezettségen alapul, a megkeresés csak akkor teljesíthető, ha az érintett ehhez – részletes tájékoztatást követően – igazolható módon hozzájárul, vagy ha az az Adatkezelő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges.

Külföldre irányuló adattovábbítás esetén az adattovábbítást végzőnek külön meg kell győződnie arról, hogy a külföldre történő adattovábbítás GDPR-ban előírt feltételei fennállnak-e. Ennek kapcsán vizsgálandó, hogy az adattovábbítás a GDPR-ban meghatározott valamely jogalapnak megfelelően történik-e, és az adatok megfelelő védelmi szintje az adatokat átvevő adatkezelőnél biztosított-e. Ha az adattovábbítás az Európai Gazdasági Térség valamely tagállamába irányul, úgy a személyes adatok megfelelő szintű védelmét nem kell vizsgálni.

Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, ha az adatkezelő és az adatfeldolgozó egyaránt teljesíti a GDPR-ban rögzített feltételeket.

Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására sor kerülhet, ha az Európai Bizottság megállapította, illetve az Európai Unió Hivatalos Lapjában és annak honlapján közzétette, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít (megfelelőségi határozat). Az ilyen adattovábbításhoz nem szükséges külön engedély.

Személyes adatok továbbítása során, amennyiben az postai küldeményként történik, biztosítani kell, hogy a küldemény zártan kerüljön feladásra.

Az Adatkezelő vállalja, hogy a személyes adatokat statisztikai célra kizárólag úgy adja át, hogy gondoskodik arról, hogy azt az érintettel ne lehessen kapcsolatba hozni.

Az Adatkezelő az általa végzett adattovábbításokat a Szabályzat 6. mellékletét képező nyilvántartás szerinti tartalommal tartja nyilván.

2.10.3. Az adatkezelési tevékenységek nyilvántartása

Az Adatkezelő köteles nyilvántartani minden olyan adatkezelési tevékenységét, amely:

a) az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár;
b) nem alkalmi jellegű;
c) különleges adatok vagy bűnügyi személyes adatok kezelésével jár.

Az Adatkezelő a fenti nyilvántartási kötelezettségének a jelen Adatkezelési Szabályzat 3. számú mellékletében foglaltak szerinti tartalommal tesz eleget.
Az Adatkezelő nevében a jelen pont szerinti nyilvántartási kötelezettségét az adatkezelést végző ügyintéző teljesíti.
A Vezérigazgató gondoskodik az adatvédelmi tevékenységek nyilvántartásának naprakészen tartásának felügyeletéről.

A Vezérigazgató köteles a nyilvántartást a NAIH ez irányú kérésére rendelkezésre bocsátani.

Az adatvédelmi tevékenységek nyilvántartása tartalmazza:

a) az Adatkezelő megnevezését és elérhetőségeit;
b) az adatkezelés megnevezését;
c) a tényleges adatkezelés helyét;
d) az adatkezelés célját;
e) az adatkezelés jogalapját;
f) az adatkezelés jogalapjának megnevezését;
g) közös adatkezelés esetén a közös adatkezelő megnevezését és elérhetőségeit;
h) az adatkezelés helyét;
i) az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét;

j) az adatkezelés technológiáját;
k) az informatikai alkalmazás megnevezését;
l) az adatkezelő által kezelt személyes adatok körét;
m) az adatkezelés időtartamát;
n) az adatok forrását;
o) adattovábbítás esetén az adatok fajtáját;
p) a címzett megnevezését és elérhetőségét;
q) a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő adattovábbítása esetén a megfelelő garanciára vonatkozó információkat;
r) az adattovábbítás jogalapját;
s) az érintettek körét;
t) az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírását. IX.

2.11. BELSŐ TRÉNINGEK, GDPR OKTATÁSOK SZERVEZÉSE ÉS AZ ADATVÉDELMI TUDATOSSÁG FEJLESZTÉSE A MUNKASZERVEZETBEN, RENDSZERES BELSŐ ADATVÉDELMI ELLENŐRZÉSI FOLYAMATOK

A Társaság az adattudatos szervezeti működés követelményének megfelelően a működése minden területén nagy hangsúlyt fektet az adatvédelmi elvek és szabályok fontosságára, és hogy ezeket a szervezetben is tudatosítsa. A GDPR 39. cikk szerint az adatvédelmi tisztviselő ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is. Amennyiben adatvédelmi tisztviselő kinevezésére nem kerül sor, a Társaság maga szervezi a személyzet adatvédelmi tudatosságának fejlesztéséhez szükséges oktatásokat/tréningeket.

2.11.1 Belső képzési struktúra

Az adatvédelmi tudatosság növelése érdekében a Társaságnál a munkakörükből fakadóan adatkezelési műveleteket végző kollégái számára az alábbi képzési és tudásról való számadási rendszert alkalmazza.

2.11.1.1. Belépéskor adatvédelmi tréning

A Társasághoz való belépést követő 10 napon belül biztosítja az adatvédelmi tudatosság kialakulását elősegítő képzést, mely az alábbi témaköröket kötelezően tartalmazza: személyes adat fogalma, adatkezelés fogalma és jogalapja, adatvédelmi kockázat, kockázatértékelés, adattudatosság a mindennapi ügyvitelben, incidensjelentési kötelezettség, a Társaság főbb adatkezelési tevékenységei.

2.11.1.2. Évente adatvédelmi tudatosságot növelő képzés

Évente egy alkalommal az adatvédelmi tudatosság szinten tartását biztosító legalább egy központilag szervezett előadáson való részvétel kötelező minden személyes adattal érintkező kolléga számára. A képzés szervezhető belső képzésként, de lehetséges a külső szolgáltató igénybevétele is.

2.11.1.3. Évente adatvédelmi felkészültség mérésére összeállított teszt

Az éves kötelező előadáson való részvételt követő 14 napon belül online kitölthető teszt formájában minden személyes adattal érintkező kollégának számot kell adnia adatvédelmi tudásáról. A teszt abban az esetben számít sikeresen teljesítettnek, amennyiben a kolléga legalább 80%-os teljesítményt ér el. Ennek megfelelően annyiszor kell kitöltenie a tesztet, amíg nem éri el a 80%-os követelményt.

2.11.2 Egyéb rendelkezések

A Társaság évente központilag, a GDPR 39. cikk (1) b) pontja szerint az adatvédelmi tisztviselő koordinálásával (ha van), illetve, ha szükséges szakértő bevonásával felülvizsgálja és aktualizálja az adatvédelmi képzési rendszer alapját képező oktatási anyagokat és az adatvédelmi tudást vizsgáló tesztet.

2.12. ADATVÉDELMI INCIDENS KEZELÉSE

Adatvédelmi incidensnek minősül 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.

Az adatvédelmi incidens megfelelő tartalmú és megfelelő időben történő intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek (és ezzel közvetve a Társaságnak). Ilyen károk lehetnek többek között a személyes adataik feletti rendelkezés elvesztése (arra jogosulatlanok hozzáférnek az adatokhoz, és nem lehet tudni, hogy később mire használják fel), a pénzügyi veszteség (pl. bankkártya adatok lopása), a jó hírnév sérelme, védett üzleti információk kiszivárgása stb.

A leggyakoribb incidensek lehetnek például: a laptop, mobil telefon, személyes adatokat tartalmazó adathordozó elvesztése, személyes adatok rossz e-mail címre küldése, személyes adatok nem biztonságos tárolása (pl. szemetesbe dobott fizetési papírok); adatok nem biztonságos továbbítása, ügyfél- és vevő- partnerlisták illetéktelen másolása, továbbítása, szerver elleni támadások, honlap feltörése.

2.12.1. Az adatvédelmi incidens észlelése

Az Adatkezelő akár belső, akár külső jelzés alapján értesülhet a nemvárt eseményről.

Belső jelzésnek minősül, ha az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személy, vagy az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozó észleli a nemvárt eseményt.

Amennyiben az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személy észleli a nemvárt eseményt, köteles haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni közvetlen felettesét, illetve az Adatkezelő vezetőjét.

Amennyiben az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló olyan személy észleli a nemvárt eseményt, akinek nincs közvetlen felettese, köteles haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni az Adatkezelő vezetőjét.

Amennyiben az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozó észleli a nemvárt eseményt, köteles az említett szerződésben meghatározott kapcsolattartó útján haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni az Adatkezelő vezetőjét.

Külső jelzésnek minősül, ha a fent meghatározott személyek körén kívül eső bármely személy észleli a nemvárt eseményt, és erről – szóban, írásban vagy elektronikus úton – tájékoztatja az Adatkezelőt.

Amennyiben a külső jelzés az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személyhez érkezik, e személy köteles haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni közvetlen felettesét, illetve az Adatkezelő vezetőjét.

Amennyiben az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló olyan személyhez érkezik a tájékoztatás, akinek nincs közvetlen felettese, köteles haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni az Adatkezelő vezetőjét.

Amennyiben az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozóhoz érkezik a tájékoztatás, köteles az említett szerződésben meghatározott kapcsolattartó útján haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni az Adatkezelő vezetőjét.

A NAIH Adatkezelő részére küldött megkeresése minden esetben külső jelzésnek minősül.

Az adatkezelő vezetője köteles a hozzá beérkezett a nemvárt eseményről szóló tájékoztatást haladéktalanul megvizsgálni. Eljárása során az alábbi tényezőket veszi figyelembe:

- a nemvárt esemény személyes adatokat érint-e;
- a nemvárt esemény a biztonság sérüléséből következett-e be;
- a biztonság sérülése milyen eredménnyel járt a személyes adatokra nézve.

Az Adatkezelő vezetője jogosult a nemvárt esemény vizsgálatával összefüggésben az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személytől, valamint az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozótól információt, tájékoztatást kérni.

Amennyiben az Adatkezelő vezetője az elvégzett vizsgálat eredményeként – megállapítja, hogy a személyes adatokat érintő nemvárt esemény a biztonság sérüléséből következett be, az a GDPR 33. cikk (1) bekezdése szerinti tudomásra jutásnak minősül.

Amennyiben az Adatkezelő vezetője a vizsgálat következtében megállapítja, hogy a nemvárt esemény adatvédelmi incidensnek minősül, köteles elvégezni az incidens kategorizálását is.

2.12.2. Az adatvédelmi incidens kivizsgálása

Az Adatkezelő vezetője haladéktalanul, legfeljebb azonban a tudomásra jutásáról számított 2 órán belül összehívja az incidenskezelő csoportot.

Az incidenskezelő csoport feladata az adatvédelmi incidens körülményeinek feltárása, az adatvédelmi incidens kockázatainak felmérése, elemzése és kezelése, valamint az adatvédelmi incidenssel kapcsolatos további intézkedések megtételére vonatkozó döntéshozatal.

Az incidenskezelő csoport vezetését és irányítását az Adatkezelő vezetője látja el.

Az incidenskezelő csoport az adatvédelmi incidens kezelésének lezárásáig folyamatosan ülésezik az Adatkezelő vezetője által meghatározott rendszerességgel.

Az incidenskezelő csoport az adatvédelmi incidens kezelésének lezárásával szűnik meg, ideértve a NAIH esetleges eljárása keretében hozott döntéseket is.

Az incidenskezelő csoport a tevékenységének lezárásaként jelen Szabályzat 8. mellékletében foglaltak szerinti formában és tartalommal jelentést készít az Adatkezelő ügyvezetőjének az incidens kezelésével kapcsolatban.

Az incidenskezelő csoport tagjai:

- IT igazgató;
- a társaság jogi képviselője;
- az érintett munkatársa;
- az Adatkezelő vezérigazgatója vagy az általa megbízott személy.

Az incidenskezelő csoport tagja lehet egyéb személy is szükség esetén.

Az incidenskezelő csoport első ülését az Adatkezelő vezetője nyitja meg.

Az Adatkezelő vezetője az incidenskezelő csoport első ülésén ismerteti az adatvédelmi incidenssel kapcsolatban rendelkezésre álló információkat, tényeket, különös tekintettel az adatvédelmi incidens bekövetkezésének körülményeire és az incidens kategorizálására.
Az incidenskezelő csoport ezt követően megkezdi az adatvédelmi incidens kockázatainak felmérését és elemzését, azok valószínűségének és súlyosságainak figyelembevételével. A kockázatok tekintetében azok forrását, a kiszolgáló környezetet, a személyes adatokat, illetve az incidens lehetséges hatásait kell vizsgálni.

(4) A kockázatok forrása tekintetében figyelembe vehető tényezők:

a) az incidens véletlen belső magatartás vagy tevékenység eredménye;
b) az incidens szándékos belső magatartás vagy tevékenység eredménye;
c) az incidens véletlen külső magatartás vagy tevékenység eredménye;
d) az incidens szándékos belső magatartás vagy tevékenység eredménye.

(5) A kiszolgáló környezet szempontjából figyelembe vehető tényezők:

a) az adatkezelés eszközei (papír alapú vagy automatizált módszerekkel történő adatkezelés);
b) az incidenssel érintett rendszer (levelező rendszer, adathordozó stb.);
c) a kiszolgáló környezet biztonságát védő intézkedések (pl. titkosítás, elnevesítés, tűzfal);
d) a kiszolgáló környezet ellenállóképessége;
e) az incidens elhárítása érdekében előzetes tett intézkedések hatékonysága;
f) az incidens bekövetkeztét lehetővé tevő tényezők;
g) az incidens bekövetkeztét befolyásoló egyéb tényezők;
h) a rendszerszerű működés helyreállításának valószínűsége.

(6) A személyes adatok szempontjából figyelembe vehető tényezők:

a) a személyes adatok kategóriái, különös tekintettel a különleges adatokra;
b) személyes adatok száma;
c) érintettek kategóriái, különös tekintettel az érintettek kiszolgáltatott helyzetéra (gyermek, munkavállaló);
d) az érintettek azonosíthatósága;
e) az érintettek száma.

(7) Az incidens hatásai szempontjából figyelembe vehető tényezők:

a) fizikai kár vagy veszély;
b) vagyoni kár;
c) nem vagyoni kár.

Az incidenskezelő csoport köteles az adatvédelmi incidenst egyedileg, kockázati szint szerint besorolni a következők szerint: alacsony, közepes vagy magas kockázatú incidens.

A (4) bekezdés b)-d) pontjaiban foglalt esetek, az (6) bekezdés a) pontjában foglalt különleges adatok és c) pontjában foglalt kiszolgáltatott helyzetben lévő érintettek, a (6) bekezdés b) pontja szerinti személyes adatok, illetve e) pontja szerinti érintettek magas száma közepes vagy magasabb kockázatot jelent.

Szintén valószínűsíthetően magasabb kockázattal jár az adatvédelmi incidens a természetes személyek jogaira és szabadságaira nézve, ha annak eredménye:

a) az érintett hátrányos megkülönböztetése;
b) személyazonosság-lopás;
c) személyazonossággal való visszaélés;
d) pénzügyi veszteség;
e) az érintett jó hírnevének sérelme;
f) a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése;
g) álnevesítés engedély nélkül történő feloldása;
h) bármilyen egyéb jelentős gazdasági vagy szociális hátrány;
i) alapvető jogai vagy szabadságai gyakorlásának ellehetetlenülése;
j) az érintettek saját személyes adatai feletti önrendelkezései jogának megszűnése;
k) személyes jellemzők értékelésére személyes profil létrehozása vagy felhasználása céljából.

Amennyiben az adatvédelmi incidens alacsony kockázatú, úgy kell tekinteni, hogy az valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Amennyiben az adatvédelmi incidens közepes kockázatú, úgy kell tekinteni, hogy az – a GDPR 33. cikk (1) bekezdése szerint – valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

Amennyiben az adatvédelmi incidens magas kockázatú, úgy kell tekinteni, hogy az – a GDPR 34. cikk (1) bekezdése szerint – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

Az incidenskezelő csoport köteles továbbá meghozni mindazon intézkedéseket, amelyek az adatvédelmi incidens következményeinek mérséklése vagy elhárítása érdekében szükséges, ideértve az érintett rendszerek működésének helyreállítását, az érintettek esetleges tájékoztatását, valamint – szabálysértés vagy bűncselekmény esetén – a szabálysértések vagy bűncselekmények felderítésére hatáskörrel és illetékességgel rendelkező szervek értesítését.

2.12.3. Az adatvédelmi incidens bejelentése

Amennyiben az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő köteles indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelentést tenni a NAIH-hoz.

Amennyiben az adatvédelmi incidens körülményeinek feltárása, kockázatainak felmérése indokolttá teszi, a bejelentés részletekben is történhet.
Az Adatkezelő nevében a bejelentési kötelezettséget a Vezérigazgató teljesíti.
A Vezérigazgató bejelentési kötelezettséget papír alapon, vagy a NAIH honlapján elérhető elektronikus bejelentési rendszer útján telesíti.

A NAIH részére tett bejelentésnek tartalmaznia kell:

a) az Adatkezelő adatait;
b) az adatvédelmi incidens időpontját;
c) az adatvédelmi incidensről való tudomásszerzés időpontját;
d) az adatvédelmi incidens észlelésének módját;
e) esetleges késedelmes tájékoztatás indokait;
f) az adatvédelmi incidens jellegét;
g) az adatvédelmi incidenssel érintett személyes adatokat;
h) az adatvédelmi incidenssel érintett személyes adatok becsült számát;
i) az érintettek kategóriáit;
j) az adatvédelmi incidens előtt alkalmazott intézkedéseket;
k) az adatvédelmi incidens következményeinek a megjelölését;
l) az érintetteket ért fizikai, anyagi vagy nem vagyoni károkat, vagy egyéb jelentős következményeket, valamint a valószínűsíthető következmények súlyosságát;
m) a megtett intézkedéseket;
n) az adatvédelmi incidens orvoslására tett intézkedéseket;
o) egyéb bejelentéseket;
p) az adatvédelmi tisztviselő nevét és elérhetőségeit.

Az Adatkezelő valamennyi munkavállalója köteles együttműködni a NAIH-hal az adatvédelmi incidensek kezelésével összefüggésben indult eljárások során.

A Vezérigazgató köteles a NAIH rendelkezésére bocsátani az adatvédelmi incidensek kezelésével összefüggésben indult eljárások lefolytatásához szükséges további információkat.

Annak érdekében, hogy a Vezérigazgató teljesíteni tudja a fenti kötelezettségét, jogosult az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személytől, valamint az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozótól információt, tájékoztatást kérni.

Az incidenskezelő csoport tagjai kötelesek közreműködni az adatvédelmi tisztviselővel a fenti kötelezettség teljesítése során.

Amennyiben az bejelentés mellőzésére kerül sor, annak okait az Adatkezelő dokumentálni köteles.

A bejelentés megtörténtével vagy mellőzésével kapcsolatos információk az incidenskezelő csoport jelentésének részét képezik.

2.12.4. Az érintettek tájékoztatása

Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő köteles indokolatlan késedelem nélkül tájékoztatni az érintettet az adatvédelmi incidensről.

Az Adatkezelő nevében az (1) bekezdés szerinti kötelezettségét az adatvédelmi tisztviselő teljesíti.

Amennyiben az adatvédelmi incidens az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személyek érint, a tájékoztatást az érintetteket foglalkoztató szervezeti egységek bevonásával, a munkavállalókkal történő kapcsolattartás céljára használt rendszerek segítségével kell megadni.

Amennyiben az adatvédelmi incidens a (3) bekezdés hatálya alá nem tartozó személyeket érint, a tájékoztatást az érintettekkel történő kapcsolattartás céljára használt rendszerek segítségével kell megadni. Ebben az esetben a tájékoztatás tartalmának kialakításában az Adatkezelő sajtókapcsolatokért felelős munkatársa közreműködik.

Amennyiben – az érintettek nagy számára tekintettel – a személyes tájékoztatás lehetetlen lenne vagy aránytalan költséggel járna az Adatkezelőre nézve, a tájékoztatás helyi vagy országos sajtótermékekben megjelentetett figyelemfelhívó jelzés útján is megadható.

Az előző két bekezdésekben foglalt esetekben az Adatkezelő honlapján figyelemfelhívó jelzést kell elhelyezni, amely általános tájékoztatást nyújt az incidens jellegéről, az érintett személyes adatok, illetve az érintettek kategóriáról.

Az érintett vagy érintettek részére nyújtott tájékoztatásnak tartalmaznia kell legalább:

a) az adatvédelmi incidens jellegének leírását;
b) az adatvédelmi tisztviselő nevét és elérhetőségeit;
c) az adatvédelmi incidens valószínűsíthető következményeinek ismertetését;
d) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések ismertetését, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is;
e) az érintettek által az adatvédelmi incidens orvoslására tehető intézkedések ismertetését, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

Annak érdekében, hogy a Vezérigazgató teljesíteni tudja a tájékoztatási kötelezettségét, jogosult az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személytől, valamint az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozótól információt, tájékoztatást kérni.

Az incidenskezelő csoport tagjai kötelesek közreműködni a Vezérigazgatóval a tájékoztatási kötelezettség teljesítése során.

Amennyiben a tájékoztatás mellőzésére kerül sor, annak okait a Vezérigazgató dokumentálni köteles.

A tájékoztatás megtörténtével vagy mellőzésével kapcsolatos információk az incidenskezelő csoport jelentésének részét képezik.

2.12.5. Az adatvédelmi incidens nyilvántartása

Az Adatkezelő köteles nyilvántartani az adatvédelmi incidenseket, tekintet nélkül azok kockázati besorolására.
Az Adatkezelő az előző bekezdés szerinti kötelezettségének a jelen szabályzat 9. számú mellékletében foglaltak szerinti formában és tartalommal tesz eleget.
Az adatvédelmi incidensek nyilvántartása tartalmazza:

a) az Adatkezelő megnevezését és elérhetőségeit;
b) az adatvédelmi incidens azonosítóját;

c) az érintett személyes adatok körét;
d) az adatvédelmi incidenssel érintettek körét;
e) az adatvédelmi incidenssel érintettek számát;
f) az adatvédelmi incidens megtörténtének időpontját;
g) az adatvédelmi incidens tudomásra jutásának időpontját;
h) az adatvédelmi incidens jellegét;
i) az adatvédelmi incidens körülményeit;
j) az adatvédelmi incidens hatásait;
k) az adatvédelmi incidens elhárítására megtett intézkedéseket;
l) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat;
m) a bejelentési kötelezettség tényét;
n) a hatósági bejelentés időpontját;
o) a bejelentő személy nevét;
p) a tájékoztatási kötelezettség tényét;
q) az érintettek tájékoztatásának időpontját;
r) a bejegyzés dátumát.

Az Adatkezelő nevében a nyilvántartási kötelezettségét a Vezérigazgató teljesíti.
A Vezérigazgató gondoskodik az adatvédelmi incidensek nyilvántartásának naprakészen tartásáról, frissítéséről.
A Vezérigazgató köteles a nyilvántartást a NAIH ez irányú kérésére rendelkezésre bocsátani.

2.13. ADATVÉDELMI HATÓSÁG ELJÁRÁSA ESETÉN KÖVETENDŐ BELSŐ SZABÁLYOK

A Társaság szervezetében a Hatósággal való megfelelő együttműködésére elsődlegesen a Vezérigazgató felel (felelős személy). Bármely a Hatóságtól érkező megkeresést a felelős személy a megkeresés beérkezését követően haladéktalanul belül köteles Vezérigazgató felé továbbítani. a Vezérigazgató a társaság jogi képviselőjével egyeztetve szükség esetén – a megkeresés taralmától függően – kezdeményezni belső munkacsoport felállítását, illetve külső szakértő bevonását.
A Hatósági megkeresésére minden esetben az előírt határidőben reagálni szükséges, mellékelve az összes a Hatóság által kért adatot/információt/dokumentumot. A Hatóság részére megküldendő bármely dokumentum tartalmát a Vezérigazgató hagyja jóvá.

1. sz. melléklet – Érdekmérlegelési Teszt nyomtatvány

ÉRDEKMÉRLEGELÉSI TESZT	
Társaság neve	
Érdekmérlegelési teszt tárgya	
Készítette (név, munkakör)	
Jóváhagyta (név, munkakör)	
A készítés időpontja	
A jóváhagyás időpontja	
Naplószám	
A tervezett adatkezelés célja	
A tervezett adatkezelés jogalapja (GDPR-megfeleltetés)	
Az adatkezeléssel érintett személyes adatok köre	
A személyes adatok forrása	
Az adatkezelés időtartama	
A Társaság által vállalt garanciák	
MEGÁLLAPÍTÁSOK	

A Társaság jogos érdeke	
Az adatkezelés szükségessége	
Az érintettek jogait és szabadságait ért sérelem	
Érdekmérlegelés	

Kelt: Budapest, 20.....

Vezérigazgató

2. sz. melléklet – Kockázatértékelés folyamata

3. számú melléklet - Adatkezelési Nyilvántartás

AZ ADATKEZELÉSI TEVÉKENYSÉGEK

Adatkezelés megnevezése	
Tényleges adatkezelés helye[1]	
Adatkezelés célja[2]	
Adatkezelés jogalapja	
Adatkezelés jogalapjának megnevezése	
Közös adatkezelő neve, címe[3]	
Adatkezelés helye[4]	
Adatfeldolgozónak az adatkezeléssel összefüggő tevékenysége[5]	
Adatkezelés technológiája[6]	
Az informatikai alkalmazás megnevezése	
Az adatkezelő által kezelt személyes adatok köre[7]	
Az adatkezelés időtartama	
Adatok forrása[8]	
Adattovábbítás esetén az adatok fajtája[9]	
Címzett neve, teljes címe[10]	
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő adattovábbítása esetén a megfelelő garanciára vonatkozó információk[11]	
Az adattovábbítás jogalapja[12]	
Érintettek köre[13]	

[1] Az Adatkezelő címének megadása (ha ettől eltérő helyen történik az adatok tárolása, akkor annak megadása).
[2] Milyen célból kellenek ezen adatok?
[3] GDPR 26. cikk.
[4] Ahol az adatfelvétel történik, vagy az adattárolás van.
[5] Ha van adatfeldolgozó akkor meg kell nevezni milyen tevékenységet látnak el. Pl.: tárhelyszolgáltatás, levelek postázása, honlapkarbantartás.
[6] Manuálisan vagy elektronikus információs rendszerrel (valamely IT alkalmazással, elektronikusan).
[7] Pl.: név, anyja neve, lakcím, e-mail cím stb.
[8] Magától az érintettől vagy 3. személytől, szervezettől érkezik az adat?
[9] Adattovábbítás esetén amikor a társaságon kívülre megy adat, akkor milyen adatok mennek (pontosan megnevezve mint a 9. pontban)?
[10] Akinek továbbítjuk az adatokat, még az adatfeldolgozó neve is itt kell, hogy szerepeljen.
[11] Megy-e harmadik országba (EU-n kívülre) személyes adat? És miért (kérjük ennek pontos megnevezését)?
[12] Pl. hozzájárulás, szerződés.
[13] Érinett, hozzátartozó, kedvezményezett, kapcsolattartó, ügyfelek.

Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása[14]	

Adatkezelés megnevezése	
Tényleges adatkezelés helye	
Adatkezelés célja	
Adatkezelés jogalapja	
Adatkezelés jogalapjának megnevezése	
Közös adatkezelő neve, címe	
Adatkezelés helye	
Adatfeldolgozónak az adatkezeléssel összefüggő tevékenysége	
Adatkezelés technológiája	
Az informatikai alkalmazás megnevezése	
Az adatkezelő által kezelt személyes adatok köre	
Az adatkezelés időtartama	
Adatok forrása	
Adattovábbítás esetén az adatok fajtája	
Címzett neve, teljes címe	
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő adattovábbítása esetén a megfelelő garanciára vonatkozó információk	
Az adattovábbítás jogalapja	
Érintettek köre	
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	

Adatkezelés megnevezése	
Tényleges adatkezelés helye	
Adatkezelés célja	
Adatkezelés jogalapja	
Adatkezelés jogalapjának megnevezése	
Közös adatkezelő neve, címe	
Adatkezelés helye	

[14] Alkalmazott adatbiztonsági intézkedések megnevezése

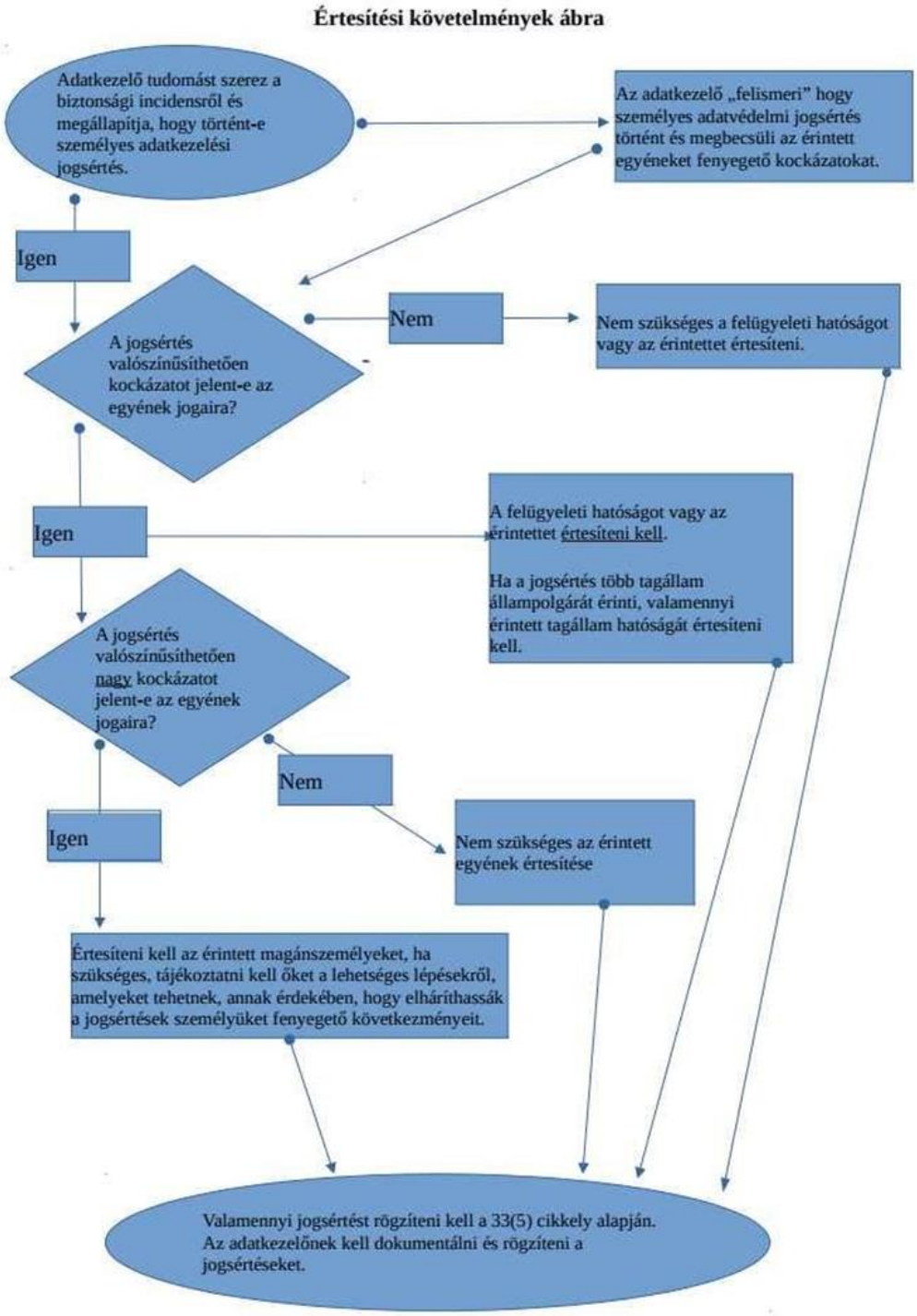
Adatfeldolgozónak az adatkezeléssel összefüggő tevékenysége	
Adatkezelés technológiája	
Az informatikai alkalmazás megnevezése	
Az adatkezelő által kezelt személyes adatok köre	
Az adatkezelés időtartama	
Adatok forrása	
Adattovábbítás esetén az adatok fajtája	
Címzett neve, teljes címe	
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő adattovábbítása esetén a megfelelő garanciára vonatkozó információk	
Az adattovábbítás jogalapja	
Érintettek köre	
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	

4. számú melléklet - Adatkezelési szabályzat

ÉRINTETTEK KÉRELMEINEK NYILVÁNTARTÁSA

№	A hozzáférési jogát érvényesíteni kívánó érintett neve, elérhetősége	Az érintett érvényesíteni kívánt hozzáférési jogának jellege (kérelem tartalma)	A jogérvényesítési kérelem benyújtásának dátuma	A hozzáférési jogát érvényesíteni kívánó érintett esetében történő adatkezelés jogalapja	A jogérvényesítési kérelem teljesítése érdekében tett intézkedés	A jogérvényesítési kérelem teljesítésének dátuma	A hozzáférési jogot korlátozó vagy megtagadó intézkedések jogi és ténybeli indokai	Bejegyzés dátuma, bejegyző aláírása
1.								
2.								

5. számú melléklet - Adatvédelmi Incidens Folyamatábra (Forrás: Adatvédelmi Munkacsoport – WP250rev01 – Iránymutatás)



6. számú melléklet

AZ ADATTOVÁBBÍTÁSOK NYILVÁNTARTÁSA

#	Személyes adatok továbbításának időpontja	Az adatszolgáltatást teljesítő szervezeti egység megnevezése	Az adattovábbítás jogalapja és célja	A továbbított személyes adatok körének meghatározása	Az adattovábbítás címzettje	Harmadik országba történt adattovábbítás	Az adatkezelést előíró jogszabályban meghatározott egyéb adatok, további megjegyzés	Bejegyzés dátuma, bejegyző neve, aláírása
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								

7. számú melléklet

Nyilatkozat az informatikai eszközök adattartalmáról az eszköz visszaszolgáltatásakor

Név: ……..……..., (anyja neve :……..……, szül. hely:……..……, szül. idő:……..……) kijelentem, hogy az EWG Rail Zártkörűen Működő Részvénytársaság (1134 Budapest, Róbert Károly körút 59.; adószám: 26242387-2-41) mint munkáltatóm a munkakörömhöz kapcsolódó feladatok elvégzése céljából az alábbi infokommunikációs eszközöket (munkahelyi számítógép, okostelefon, egyéb informatikai és infokommunikációs eszköz) biztosította számomra

eszköz megnevezése:	azonosító:
……	
……	
……	
……	
……	

Nyilatkozom arról, hogy a fenti eszközökön kizárólag a munkafeladatokkal összefüggő adatok találhatók.

Kelt: ……,……..……

…….

munkavállaló

A nyilatkozatot az EWG Rail Zártkörűen Működő Részvénytársaság megbízásából átvettem:

Kelt: ……,……..……

…… ……

név aláírás

8. számú melléklet

JEGYZŐKÖNYV

ADATVÉDELMI INCIDENS KEZELÉSÉRŐL

Értekezlet részletei	
Az értekezlet neve és célja:	**Adatvédelmi Bizottság, adatvédelmi incidens vizsgálata**
Dátum és helyszín:	
Jegyzőkönyv száma:	
Jegyzőkönyvvezető:	
Résztvevők neve	**Résztvevők munkaköre**

1. **Előzmények:**

2. **Az esemény besorolása**

- A leírtak alapján megállapítható, hogy adatvédelmi incidens történt /nem történt, (indok: …)

3. **Adatvédelmi incidens jellemzői:**

- Az érintettek jellege:
- Az érintettek száma:
- Sérülés jelleg:
- Adatvédelmi incidens jellege:
- Adatvédelmi incidens oka:
- Az adatvédelmi incidens körülményei és hatásai:
- Az adatvédelmi incidens előtt alkalmazott intézkedések leírása:
- Az adatvédelmi incidens következményei:
- Az érintett személyes adatok jellege:

4. Megállapítások és javaslatok

Tekintettel az adatvédelmi incidens jellegére és súlyossági fokára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira, az Adatvédelmi Bizottság úgy határozott, hogy szükséges /nem szükséges bejelentést tenni az Adatvédelmi Hatóság felé, az adatvédelmi incidens magas kockázattal jár /nem jár az érintettek jogaira és szabadságaira, azaz a magánszférájukra.

5. Az Adatvédelmi Bizottság javaslatai:

a) …
Felelős: …

b) A kockázatok enyhítése körében:
Felelős: …

c) Egyéb
Felelős: ….

d) A határidő a megtett intézkedésekről:…

Kelt:

……..	……..	……..
név, munkakör	név, munkakör jegyzőkönyvvezető	név, munkakör

……..
név, munkakör

9. számú melléklet – Adatvédelmi incidens nyilvántartás

ADATVÉDELMI INCIDENSEK

Sorszám[15]	
Az érintett személyes adatok köre[16]	
Az adatvédelmi incidenssel érintettek köre[17]	
Az adatvédelmi incidenssel érintettek száma	
Az adatvédelmi incidens megtörténtének időpontja	
Az adatvédelmi incidens tudomásra jutásának időpontja	
Az adatvédelmi incidens jellege	
Az adatvédelmi incidens körülményei	
Az adatvédelmi incidens hatásai	
Az adatvédelmi incidens elhárítására megtett intézkedések	
Az adatkezelést előíró jogszabályban meghatározott egyéb adatok	
Kell-e a NAIH-nak bejelenteni?	
Hatósági bejelentés időpontja	
Bejelentő személy neve	
Kell-e tájékoztatni az érintetteket?	
Érintettek tájékoztatásának időpontja	
Bejegyzés dátuma (év, hónap, nap)	

Sorszám	
Az érintett személyes adatok köre	
Az adatvédelmi incidenssel érintettek köre	
Az adatvédelmi incidenssel érintettek száma	

[15] Minden egyes incidens esetében kitöltendő!
[16] Pl.: név, anyja neve, lakcím, e-mail cím stb.
[17] Pl. munkavállaló stb.

Az adatvédelmi incidens megtörténtének időpontja	
Az adatvédelmi incidens tudomásra jutásának időpontja	
Az adatvédelmi incidens jellege	
Az adatvédelmi incidens körülményei	
Az adatvédelmi incidens hatásai	
Az adatvédelmi incidens elhárítására megtett intézkedések	
Az adatkezelést előíró jogszabályban meghatározott egyéb adatok	
Kell-e a NAIH-nak bejelenteni?	
Hatósági bejelentés időpontja	
Bejelentő személy neve	
Kell-e tájékoztatni az érintetteket?	
Érintettek tájékoztatásának időpontja	
Bejegyzés dátuma (év, hónap, nap)	

Hatályba léptető rendelkezés:

A jelen szabályzat 2024. augusztus 30. napján lép hatályba.

Vezérigazgató aláírásával 2024. augusztus 30. napján jóváhagyta.

Dokumentum kiadása

Készítette: Dr. Fridman Róbert Ügyvédi Iroda

Dr. Fridman Róbert Ügyvédi Iroda
Dr. Fridman Róbert
ügyvéd
1054 Budapest, Bank u. 5. 1. em. 2.
Tel/Fax: 800-9094

Jóváhagyta:

EWG Rail Zrt. 1.
1134 Budapest, Róbert Károly krt. 59.
Adószám: 26242387-2-41
Cégj.sz.: 01-10-049688

_____

EWG Rail Zrt. képviseletében: Miskolczi Gábor Vezérigazgató