

Azonosító: .../2025.	Tárgy: A Magyar Vagon csoport adatvédelmi szabályzatáról		Hatályba lép: 2025.
	Oldal:	Kiadva: 2025.	

Magyar Vagon csoport

.../2025. sz. Csoportszintű Szabályzata A Magyar Vagon csoport adatvédelmi szabályzatáról

Jóváhagyta és kiadta:	Jóváhagyta és kiadta:
.....
Dr. Ludvig László CEO	Tamás Lóránd CFO

Készítette:
.....
Dr. Jamrik Zsófia CLO

MÓDOSÍTÁSOK JEGYZÉKE		
Sorszám	Módosítás leírása	Változat/dátum

TARTALOMJEGYZÉK

1.0	AZ UTASÍTÁS CÉLJA	3
2.0	HATÁLY ÉS FELELŐSSÉG MEGHATÁROZÁSA	3
2.1	Az utasítás hatálya.....	3
2.1.1	Az utasítás személyi hatálya	3
2.1.2	Az utasítás tárgyi hatálya	3
2.2	Az utasítás kidolgozásáért és karbantartásáért felelős	3
3.0	FOGALMAK MEGHATÁROZÁSA	3
4.0	AZ UTASÍTÁS LEÍRÁSA	5
4.1	A személyes adat kezelésének általános szabályai	6
4.1.1	A személyes adatok kezelésének alapelvei	6
4.1.2	A személyes adatok kezelésének jogalapjai	7
4.1.3	Érintettek jogainak biztosítása	9
4.1.4	Adatkezelő és adatfeldolgozó.....	14
4.2	Általános feladatok, felelősségek és hatáskörök	16
4.3	Feladatok és felelősségek az adatkezelés megkezdése előtt	17
4.3.1	Az Adatkezelő szervezeti egység feladata	17
4.3.2	A Biztonsági szervezet információbiztonsági szakértőjének feladata	24
4.4	Feladatok és felelősségek a személyes adatok kezelése során	24
4.4.1	Az Adatkezelő szervezeti egység feladata	24
4.4.2	A biztonsági vezető feladatai	25
4.4.3	A Biztonsági szervezet információbiztonsági szakértőjének feladata	26
4.4.4	Informatika szervezet	26
4.5	Az adatkezelés lezárása	26
4.5.1	Az Adatkezelő szervezeti egység feladata	26
4.5.2	A biztonsági vezető feladata	27
5.0	HIVATKOZÁSOK, MÓDOSÍTÁSOK HATÁLYON KÍVÜL HELYEZÉSEK	27
5.1	Hivatkozások	27
5.2	Módosítások	27
5.3	Hatályon kívül helyezések	27
5.4	Magyar Vagon Business Solutions Kft. tájékoztatása	27
5.5	Rendelkezések	27
6.0	HATÁLYBA LÉPTETÉS	27
7.0	MELLÉKLETEK, BIZONYLATOK	27
7.1	Mellékletek	27
7.2	Bizonylatok	28

1.0 AZ UTASÍTÁS CÉLJA

Az utasítás célja, hogy meghatározza a Magyar Vagon csoportba tartozó gazdasági társaságok tevékenységével összefüggésben a Társaság birtokába kerülő személyes adatok kezelésének és azok nyilvántartásának rendjét, biztosítsa az adatbiztonság követelményeinek érvényesülését, illetve megteremtse a személyes adatok szabad áramlásához szükséges feltételeket, a vonatkozó jogi szabályozás tükrében.

Fentiek teljesülése érdekében jelen utasítás a Magyar Vagon csoportba tartozó gazdasági társaságok adatvédelmi szabályozási struktúrájának tetején foglal helyet.

2.0 HATÁLY ÉS FELELŐSSÉG MEGHATÁROZÁSA

2.1 Az utasítás hatálya

2.1.1 Az utasítás személyi hatálya

Az utasítás személyi hatálya kiterjed valamennyi Magyar Vagon csoportba tartozó társaságra, azok valamennyi szervezeti egységére, munkavállalójára, valamint a társaságokkal szerződéses jogviszonyban álló természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre, a velük kötött szerződésekben, illetve – amennyiben az adott jogviszony kapcsán létrejött ilyen nyilatkozat, akkor – a titoktartási nyilatkozatokban rögzített mértékig.

2.1.2 Az utasítás tárgyi hatálya

Az utasítás tárgyi hatálya kiterjed a társaságok szervezeti egységeinél, vagy a társaságokkal szerződéses jogviszonyban álló adatfeldolgozóknál folytatott minden olyan adatkezelésre és adatfeldolgozásra, amely a társaságok által kezelt személyes adatra vonatkozik, függetlenül attól, hogy az adatkezelés, illetve adatfeldolgozás teljesen, vagy részben automatizált eszközzel, vagy manuálisan történik.

2.2 Az utasítás kidolgozásáért és karbantartásáért felelős

Az utasítás elkészítéséért és szükség szerinti módosításáért a Magyar Vagon Befektetési Vagyonkezelő Zrt. jogi vezetője felelős.

3.0 FOGALMAK MEGHATÁROZÁSA

Adatbázis: logikailag összetartozó, többnyire strukturált adatok összessége, amelyet az adatok gyűjtésére, felvételére, rögzítésére, rendszerezésére, tárolására, megváltoztatására, felhasználására, lekérdezésére, továbbítására, összehangolására vagy összekapcsolására, zárolására, törlésére alkalmas szoftvereszköz kezel. Az adatbázis lényege, hogy az adatok mellett az adatok között lévő kapcsolatokat is tárolja;

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.

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.

Adatkezelő szervezeti egység: a társaságok azon SZMSZ szerinti szervezeti egysége, amely az adatkezelést az adott társaság képviselőjében végzi.

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

Adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

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

Adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

Adatmegsemmítés: az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Adattörléshez való jog („elfeledtetéshez való jog”): Az érintett joga arra, hogy kérésére az adatkezelő a jogszabályban meghatározott esetekben indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat.

Adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.

Adatvédelem: a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozását, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

Adattovábbítás: az adat meghatározott harmadik fél számára történő hozzáférhetővé tétele.

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.

Automatizált döntéshozatal: amikor a személyes adatok kezelése során folytatott eljárás az érintettre nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti és a döntéshozatalra technológiai eszközökkel, emberi beavatkozás nélkül kerül sor.

Anonimizálás: az érintettől kezelt személyes adatok olyan módon történő szűkítése, amelynek következtében az adat elveszíti a személyes adat jellegét, azaz többé már sem közvetlenül sem közvetett módon, még további információk hozzáadásával sem állapítható meg, hogy korábban mely természetes személyre vonatkozott. Az anonim adatra nem alkalmazandók a személyes adatok védelmére vonatkozó szabályok.

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

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.

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

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

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

Érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy.

GDPR: az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről.

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

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

Harmadik ország: minden olyan állam, amely nem EGT-állam.

Hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), mely független szervként a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését ellenőrzi.

Magyar Vagon csoport: a Magyar Vagon Befektetési Vagyonkezelő Zrt. és kapcsolatos vállalkozásai. A jelen Szabályzat hatálybalépésének napján ezek a Magyar Vagon Befektetési Vagyonkezelő Zrt., a Ganz-MaVag Holding Kft., a Ganz-MaVag Europe Kft., a Ganz-MaVag Invest Zrt., Ganz-MaVag International Kft., a Magyar Vagon Business Solutions Kft., a Dunakeszi Járműjavító Kft. és a Magyar Vagon Vasúti Járműgyártó, Javító és Karbantartó Kft. (a továbbiakban: Társaság vagy Társaságok).

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik.

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

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

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

Személyes adatok különleges kategóriái: 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.

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

4.0 AZ UTASÍTÁS LEÍRÁSA

A Társaságok üzleti szereplőként tevékenységi körükben eljárva különösen ügyfeleinek-, valamint üzleti partnereinek jelentős mennyiségű személyes adata kezeléséért felelős.

A Társaságok, mint munkáltatók kezelik a munkavállalóiknak- és azok családtagjainak személyes adatait is.

Személyes adat kezelésére csak jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség. A Társaságok által kezelt személyes adatok magáncélra való felhasználása tilos.

Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének.

Az utasításban előírtak betartásáért a feladatkörében minden érintett szervezeti egység vezetője felelős.

A személyes adatok kezelésének megtervezésekor figyelemmel kell lenni arra, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

A Társaságok munkatársai munkájuk során kötelesek gondoskodni arról, hogy jogosulatlan személyek ne férhessenek hozzá személyes adatokhoz.

A Társaságok szervezeti egységeinél adatkezelést végző munkavállalók és a Társaságok megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek munkavállalói kötelesek a megismert személyes adatokat megőrizni. A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek Titoktartási nyilatkozatot tenni.

Ha az utasítás hatálya alatt álló személy tudomást szerez arról, hogy az érintett Társaság által kezelt személyes adat hibás, hiányos vagy időközben megváltozott, haladéktalanul köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni. Az adatvédelmi jogszabályoknak való megfelelés érdekében a Társaságoknak

- az adatkezeléseit úgy kell megterveznie, hogy azok megfeleljenek az adatvédelem alapelveinek,
- a személyes adatok kezelése alapelveinek az adatkezelés teljes folyamatában érvényesülniük kell, valamint
- az adatkezelés teljes folyamatának leteltével, az adatkezelés céljának megvalósulásával, a személyes adatokat törölni, vagy anonimizálni kell.

A személyes adatkezelés, adatfeldolgozás során az abban résztvevők között a kommunikáció (pl. tájékoztatás, tanácsadás) generális szabályként írásban történik (ideértve az elektronikus levelezést is).

4.1 A személyes adat kezelésének általános szabályai

Az utasítás jelen 4.1. pontja a Társaságok, mint Adatkezelők legfontosabb feladatait általánosságban írja le. Ezek a feladatok a konkrét adatkezeléssel járó folyamatok tekintetében automatikusan delegálásra kerülnek az adott adatkezelő szervezeti egység felelősségi és feladatkörébe. Az adatkezelő szervezeti egységek konkrét feladatai a 4.2-es ponttól a 4.4-es pontig kerülnek kifejtésre. Ezen pontok helyenként visszautalnak az utasítás általános részéhez, de a feladatok és felelőségek továbbra is az adott folyamatért felelős adatkezelő szervezeti egységet terhelik.

4.1.1 A személyes adatok kezelésének alapelvei

A személyes adatok kezelésének minden szakaszában érvényesülnie kell, az alábbi alapelveknek:

A jogszerűség-, tisztességes eljárás- és átláthatóság elvének való megfelelés érdekében a személyes adatok kezelésére csak meghatározott jogalap megléte esetén kerülhet sor. A személyes adatokat tisztességesen és az érintett által átlátható módon kell kezelni. Az adatkezeléssel kapcsolatos információkat pontos, átlátható, könnyen hozzáférhető formában, egyszerű és érthető nyelvezettel kell megadni.

A célhoz kötöttség elvének megfelelően a Társaságok személyes adatot csak meghatározott, jogszerű célból, jog gyakorlása vagy kötelezettség teljesítése érdekében kezelhetnek, a cél eléréséhez szükséges minimális mértékben és ideig. Az adatkezelés minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatokat törölni kell.

Az adattakarékosság elvének érvényesüléséhez az adatgyűjtés és az adatkezelés során az a legszűkebb adatkör kezelhető, amellyel az adatkezelés előre meghatározott célja elérhető, ennél több adatot-, vagy a cél megvalósításához alkalmatlan adatot kezelni tilos.

A pontosság elvének való megfelelés érdekében gondoskodni kell arról, hogy az adatok naprakészsége biztosítva-, adott esetben az adatok rendszeres, vagy változás esetén történő frissítése garantálva legyen. A pontatlan személyes adatokat haladéktalanul törölni vagy helyesbíteni kell.

A **korlátozott tárolhatóság** elvének való megfelelés érdekében a lehető legpontosabb mértékben előre meg kell határozni az adatok tárolásának idejét, úgy, hogy az adatok csak az adatkezelés céljainak eléréséhez szükséges ideig legyenek az érintettekhez köthetők.

Biztosítani kell, hogy az adatok az adatkezelés időtartamának lejártát követően további, személyhez nem köthető felhasználás esetén anonimizálásra vagy minden más esetben automatikusan, vagy mechanikusan törlésre kerüljenek.

Az **integritás és bizalmas jelleg** elvének megfelelően az Adatkezelő az adatkezelést úgy alakítja ki, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága. Gondoskodnia kell az adatok jogosulatlan vagy jogellenes kezelésének megakadályozásáról, illetve biztosítania kell a véletlen elvesztés, megsemmisítés vagy károsodás elleni védelmet.

Az **elszámoltathatóság** elvének való megfelelés keretében a Társaságokra hárul annak felelőssége, hogy a fent felsorolt elveknek megfeleljen az adatkezelés teljes folyamata, ebből adódóan a Társaságoknak képesnek kell lennie a megfelelés igazolására. A megfelelés igazolása érdekében a Társaságok az adatkezeléssel járó szakmai folyamatait érintő belső szabályzataiban ki kell, hogy térjen az adatok kezelésével kapcsolatos valamennyi körülményre.

4.1.2 A személyes adatok kezelésének jogalapjai

A Társaságoknál személyes adat csak a GDPR 6. cikk (1) bekezdésében foglaltak alapján, míg a személyes adatok különleges kategóriájába tartozó személyes adat csak a GDPR 9. cikkben foglaltak alapján, az alábbiak szerint kezelhető.

4.1.2.1 A személyes adatok kezelésének jogalapjai

Az érintett (kifejezett) hozzájárulása

Az érintett hozzájárulásán alapuló adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, írásbeli – ideértve az elektronikus úton tett –, vagy szóbeli nyilatkozattal előzetes hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez. A hozzájárulás csak önkéntes lehet, ezáltal kizárólag akkor jogszerű, ha az érintett azt nem kényszer alatt adja meg, illetve annak elmaradása rá nézve hátrányos következményekkel nem járhat. A hozzájárulást az adatkezelőtől kapott konkrét, és megfelelő tájékoztatásnak kell megelőznie.

Az elszámoltathatóság elvéből következően, ha az adatkezelés hozzájáruláson alapul, az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult. Ezért a hozzájárulásnak dokumentálnak, és visszakereshetőnek kell lennie. Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja, amely más ügyekre is vonatkozik, a hozzájárulási nyilatkozatot egyértelműen el kell különíteni az egyéb tartalomtól, nyelvezetének egyszerűnek és világosnak kell lennie.

Az Adatkezelőnek az érintett hozzájárulását adatkezelési célonként kell elkérnie. Ha egy adatkezelésnél több adatkezelési célt szükséges megjelölni, akkor az Adatkezelőnek úgy kell kialakítania a hozzájáruló nyilatkozatot, hogy az érintett célonként külön-külön tudja megadni hozzájárulását.

Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely nincs összhangban a GDPR rendelkezéseivel, kötelező erővel nem bír.

Az érintett hozzájárulását bármikor visszavonhatja, erre az adatkezelőnek egyszerű lehetőséget kell biztosítania. A hozzájárulás visszavonása nem érinti a visszavonás előtti adatkezelés jogszerűségét, erről az érintettet a hozzájárulást megelőzően tájékoztatni kell.

A közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában hozzájárulás alapján végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét betöltött kiskorú gyermek, mint érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezeléséhez szülői hozzájárulás, illetve engedély

szükséges, kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló személy adta meg, illetve engedélyezte.

Szerződés teljesítése

Az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. Ez a jogalap elsősorban az Adatkezelő és az érintett Társaság üzleti partnerei, munkavállalói közt létrejött szerződés keretében megvalósuló, vagy ahhoz kapcsolódó személyes adatkezelések esetén alkalmazandó.

Jogi kötelezettség teljesítése

Az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. Ezt az adatkezelő elsősorban akkor alkalmazhatja, ha az adatok kezelését jogszabály kifejezetten előírja, vagy ha az érintett(ek) jogaira nézve megfelelő garanciákról rendelkező jogszabály lehetőséget biztosít annak alkalmazására.

Az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme

Az adatkezelés az érintett vagy másik természetes személy létfontosságú érdekeinek védelmében történik. Más természetes személy létfontosságú érdekeire hivatkozással személyes adatkezelésre elvben csak akkor kerülhet sor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető.

Közérdekű feladat végrehajtása

Az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges. Ebben az esetben az adatkezelésnek jogszabályban foglalt jogalappal kell rendelkeznie.

Jogos érdek érvényesítése

Az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges. Fontos kitétel, hogy ezen jogalap alkalmazása csak akkor lehetséges, ha az adatkezelő vagy harmadik fél jogos érdekei elsőbbséget élveznek az érintett érdekei vagy alapvető jogai és szabadságaival szemben, amelyek személyes adatok védelmét teszik szükségessé. Az adatkezelő a jogos érdek alátámasztása érdekében érdekmérlegelési tesztet végez.

4.1.2.2 Személyes adatok különleges kategóriái

A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, 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 kezelése a Társaságoknál kizárólag akkor lehetséges, ha

- az érintett kifejezett hozzájárulását adta az említett személyes adatok kezeléséhez, és azt jogszabály kifejezetten nem tiltja,
- a foglalkoztatást, szociális biztonságot és védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges,
- az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, és az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni,
- az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;
- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott,
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges,
- az adatkezelés jelentős közérdek miatt szükséges, megfelelő garanciákat biztosító jogszabályi háttér megléte esetén,

- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges,
- az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan vagy;
- az adatkezelés a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

4.1.2.3 A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése

A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok kezelésére kizárólag abban az esetben kerülhet sor, ha az adatkezelést az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó jogszabály lehetővé teszi.

4.1.3 *Érintettek jogainak biztosítása*

A Társaságoknak a személyes adatok kezelésének teljes szakaszában biztosítani kell az érintetti jogok gyakorolhatóságát.

4.1.3.1 Általános szabályok

A Társaságoknak úgy kell megvalósítani az érintett tájékoztatását, hogy az érintett részére a személyes adatok kezelésére vonatkozó tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. A tájékoztatás nyelvezetének mindig igazodnia kell az érintettek köréhez. A tájékoztatást írásban vagy egyéb, megtörténtének bizonyítására alkalmas módon kell biztosítani.

A Társaságoknak az adatkezelést úgy kell kialakítani, hogy adott esetben biztosítható legyen az érintett hozzáférési-, helyesbítéshez és törléshez való-, az adatkezelés korlátozásához való-, az adathordozhatósághoz való-, a tiltakozáshoz való-, és az automatizált döntéshozatallal kapcsolatban felmerülő jogainak gyakorolhatósága.

A Társaságoknak az érintettek kérelmére indokolatlan késedelem nélkül, a kérelem kézhezvételétől számított egy hónapon belül tájékoztatnia kell az érintettet a kérelme nyomán megtett intézkedésekről. A határidő a kérelem összetettségére és a kérelmek számára való tekintettel, egy alkalommal legfeljebb további két hónappal meghosszabbítható. Az érintettet a kézhezvételtől számított egy hónapon belül tájékoztatni kell a meghosszabbítás tényéről és annak okáról.

A Társaságoknak, a kérelem elektronikus úton történő beérkezése esetén, elsősorban elektronikus úton kell azt megválaszolniuk, amelytől eltérni akkor lehet, ha az érintett azt kifejezetten másként kéri. A megválaszolás tényének azonban minden esetben bizonyíthatónak kell lennie.

Ha az érintett Társaság nem tesz intézkedéseket az érintett kérelme nyomán, úgy késedelem nélkül, de legkésőbb a kérelem kézhezvételétől számított egy hónapon belül tájékoztatnia kell az érintettet az intézkedés elmaradásának okairól, valamint a bírósági jogorvoslat-, illetve a Hatósághoz fordulás lehetőségéről.

A Társaságoknak az érintett tájékoztatását és jogainak gyakorlását díjmentesen kell biztosítani. Ez alól kivételt jelent, ha az érintett kérelme egyértelműen megalapozatlan, vagy – különösen ismétlődő jellege miatt – túlzó. Ebben az esetben a Társaságok figyelemmel az adminisztratív költségekre, észszerű összegű díjat számíthatnak fel, vagy megtagadhatják a kérelem alapján történő intézkedést.

A megalapozatlan vagy túlzó jelleg bizonyítása az érintett Társaságot terheli. A megalapozatlan vagy túlzó jelleget egyedileg kérelmenként kell megállapítani. Túlzó jellegű lehet a kérelem, ha folyó évben azonos adatkörre vonatkozóan az érintett már nyújtott be kérelmet. A már megfizetett költségtérítést az érintett Társaság vissza kell, hogy térítse, amennyiben az adatokat jogellenesen kezelte, vagy a tájékoztatás kérése helyesbítéshez vezetett.

Az érintetti jogok biztosításának és az annak során esetlegesen felmerülő költségtérítés megállapításának folyamata:

- A Társasághoz beérkezett igényt az azt fogadó szervezeti egység haladéktalanul köteles továbbítani a biztonsági vezető és az érintett Adatkezelő szervezeti egység részére.
- A Társaság Adatkezelő szervezeti egységének – figyelemmel a személyes adatok kezelésére vonatkozó alapelvekre – mérlegelnie kell, hogy a kérés megalapozatlan vagy túlzó jellegű-e, másolatkérési jog teljesítése esetén pedig azt, hogy első alkalommal történik-e az igénylés.
- Amennyiben az igény teljesítésre kerül, a Társaság Adatkezelő szervezeti egységének – figyelemmel a személyes adatok kezelésére vonatkozó alapelvekre – össze kell gyűjtenie a kérés teljesítéséhez szükséges anyagköltséget és ráfordítandó munkaóra költségét.
- A Társaság Adatkezelő szervezeti egységének a kérés teljesítéséhez szükséges adminisztratív költségről tájékoztatnia kell az érintettet.
- Az érintett részéről történő költség elfogadása esetén a Társaság Adatkezelő szervezeti egységének teljesítenie kell az érintett kérését és tájékoztatnia kell a biztonsági vezetőt.

Amennyiben a Társaság nem tudja beazonosítani a jogaival élni kívánó érintettet, akkor további, a beazonosításra alkalmas adatokat kell bekérnie tőle.

4.1.3.2 Az érintett tájékoztatása

Az érintett tájékoztatása kétféleképpen történhet:

- I. az egyik esetben a Társaság a személyes adatokat közvetlenül az érintettől,
- II. a másik esetben nem az érintettől szerzi be.

I. Ha az érintettre vonatkozó személyes adatok beszerzése közvetlenül az érintettől történik, a Társaságnak a legkésőbb az adatok beszerzésének időpontjában,

a) tájékoztatnia kell az érintettet:

- a Társaság megnevezéséről, valamint kapcsolattartás céljából fenntartott elérhetőségekről,
- az adatvédelmi feladatok ellátásával megbízott munkavállaló elérhetőségeiről,
- az adatkezelés céljáról és jogalapjáról,
- amennyiben az adatkezelés jogos érdeken alapul, a Társaság vagy harmadik fél jogos érdekeiről,
- adattovábbítás esetén, annak címzettjeiről, illetve a címzettek kategóriáiról,
- harmadik országba történő adattovábbítás esetén, annak tényéről, valamint az GDPR-ban meghatározott egyéb körülményeiről.

b) a tisztességes és átlátható adatkezelés elvének való megfelelés érdekében a tájékoztatónak információval kell szolgálnia:

- a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól,
- az érintett azon jogáról, hogy kérelmezheti a Társaságtól a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogának gyakorlásáról,
- a hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jogáról, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
- felügyeleti hatósághoz címzett panasz benyújtásának jogáról,
- arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e a személyes adatokat

megadni, továbbá, hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása,

- automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról és arra vonatkozóan érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Amennyiben a Társaság a személyes adatokat a gyűjtésük céljától eltérő célból kívánja kezelni, az új adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról, továbbá a jelen I. b) pontban felsorolt adatkezelési körülményekről.

II. Ha az érintettre vonatkozó személyes adatok beszerzése nem az érintettől történik, a Társaságnak

a) tájékoztatnia kell az érintettet:

- a Társaság megnevezéséről, valamint kapcsolattartás céljából fenntartott elérhetőségekről,
- az adatvédelmi feladatok ellátásával megbízott munkavállaló elérhetőségeiről,
- az adatkezelés céljáról és jogalapjáról,
- az adatkezelésben érintett személyes adatok kategóriáiról,
- adattovábbítás esetén, annak címzettjeiről, illetve a címzettek kategóriáiról,
- harmadik országba történő adattovábbítás esetén, annak tényéről, valamint az GDPR-ban meghatározott egyéb körülményeiről.

b) továbbá a tisztességes és átlátható adatkezelés érdekében a tájékoztatónak információval kell szolgálnia:

- a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól,
- amennyiben az adatkezelés jogos érdeken alapul, a Társaság vagy harmadik fél jogos érdekeiről,
- az érintett azon jogáról, hogy kérelmezheti a Társaságtól a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról,
- a hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jogáról, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
- felügyeleti hatósághoz címzett panasz benyújtásának jogáról,
- az adatok forrásáról, adott esetben a nyilvános forrásra külön ki kell térni,
- automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról és arra vonatkozóan érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

A Társaságnak az érintett tájékoztatását úgy kell megvalósítania, hogy az a személyes adatok kezelésének konkrét körülményeit figyelembe véve, a személyes adatok megszerzésétől számított ésszerű határidőn, de legkésőbb egy hónapon belül megtörténjen. Ezen a határidőn belül, ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával, illetve, ha várhatóan más címmel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor kell megadni a tájékoztatást.

Amennyiben a Társaság a személyes adatokat a gyűjtésük céljától eltérő célból kívánja kezelni, az új adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról, továbbá a jelen II./b) pontban jelzett adatkezelési körülményekről.

A Társaságnak nem kell tájékoztatnia az érintettet, amennyiben

- az érintett már rendelkezik az információkkal, vagy
- az információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy
- aránytalanul nagy erőfeszítést igényelne, vagy
- valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné az adatkezelés céljainak elérését.

Előbbi esetekben az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, a Társaságnak megfelelő intézkedéseket kell hoznia, például a tájékoztatás nyilvános elérhetőségének biztosításával.

A Társaság tájékoztatási kötelezettsége szintén nem áll fenn, amennyiben a személyes adat megszerzését, vagy közlését kifejezetten előírja jogszabály, amely az érintett jogos érdekét szolgáló intézkedésekről külön rendelkezik, vagy ha a személyes adatoknak valamely jogszabályban előírt titoktartási kötelezettség alapján bizalmasnak kell maradniuk.

Hatósági ajánlás által támasztott további tájékoztatási kötelezettség

A Hatóság által kibocsátott ajánlás értelmében mind az I., mind pedig a II. pont esetén az érintetteknek szóló tájékoztatást ki kell egészíteni

- az adatok megismerésére jogosult személyek körével,
- adatbiztonsági intézkedésekről szóló tájékoztatással.

4.1.3.3 Hozzáférés, helyesbítés, törlés, korlátozás, adathordozhatóság, és tiltakozás

A Társaságoknak gondoskodniuk kell arról, hogy az alábbiakban részletezett érintetti jogokat a 4.1.3.1-es, általános szabályokat leíró fejezetben foglaltaknak megfelelően biztosítsák.

Hozzáférési jog

Ha az érintett a Társasághoz eljuttatott kérelmében, hozzáférési jogával kíván élni, akkor a Társaság tájékoztatja arról, hogy személyes adatainak kezelése folyamatban van-e. Amennyiben folyamatban van, úgy a Társaság az érintett személyes adataihoz hozzáférést biztosít, valamint tájékoztatást nyújt

- az adatkezelés céljairól,
- a személyes adatok kategóriáiról,
- az adattovábbítás címzettjeiről,
- az adatok tárolásának időtartamáról,
- arról, hogy adott esetben kérheti a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen,
- Hatósághoz benyújtható panasz jogáról,
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információról,
- automatizált döntéshozatal tényéről, beleértve a profilalkotást is, valamint az ezekben az esetekben alkalmazott logikáról, és arról, hogy adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

Amennyiben a Társaság a személyes adatokat harmadik országba továbbítja, tájékoztatást nyújt a GDPR-ban foglalt egyéb garanciák meglétéről.

A Társaságnak biztosítania kell az érintett másolatigénylési jogának gyakorolhatóságát. A másolatot első alkalommal ingyenesen kell az érintett rendelkezésére bocsátani, további másolatokért adminisztratív költségeket lehet felszámítani. Adminisztratív költségként a kérés teljesítésére fordított munkaóra és a tényleges anyagköltség vehető figyelembe. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

Helyesbítéshez való jog

A Társaságok az adatkezelést úgy alakítják ki, hogy az érintett kérelme esetén indokolatlan késedelem nélkül helyesbíteni tudják a rá vonatkozó, pontatlanul tárolt személyes adatokat, hiányos adatok esetén pedig az érintettől beszerezzék a személyes adatokat, úgy, hogy a tájékoztatás és a hozzájárulás is megvalósuljon.

Törléshez való jog

Az érintett jogosult arra, hogy kérésére a Társaság indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat. A Társaság köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha

- az adatkezelés célja megszűnt,
- az érintett visszavonja hozzájárulását, és más jogalap nincs az adatok kezelésére,
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
- a személyes adatokat jogellenesen kezelik,
- hozzájáruláson alapuló, közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelésére vonatkozik.

Amennyiben a Társaság által már nyilvánosságra hozott személyes adatokra vonatkozik az érintett megalapozott törlési igénye, akkor a technológia és a megvalósítás költségeit mérlegelve, a Társaságnak meg kell tennie 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.

A törléshez való jogot korlátozhatja a véleménynyilvánítás szabadságához való jog, a jogi kötelezettség, a közérdek (közérdekű és a közérdekből nyilvános adatok kezelése), illetve, ha az adatkezelés szükséges a jogi igények előterjesztéséhez, érvényesítéséhez, valamint védelméhez. A törléshez való jog korlátozhatósága esetenként mérlegelendő. A törléshez való jog korlátozhatóságának elbírálásakor a biztonsági vezető véleményét ki kell kérni.

Korlátozás

A Társaságnak az érintett kérésére korlátoznia kell az adatkezelést, az alábbi esetekben:

- az érintett vitatja az adatok pontosságát, ekkor azok ellenőrzésének idejére kell korlátozni az adatkezelést,
- az adatkezelés jogellenes, és az érintett az adatok törlése helyett, azok felhasználásának korlátozását kéri,
- az adatkezelés célja megszűnt, 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 a Társaság jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A Társaságnak biztosítania kell, hogy a korlátozás alatt álló adatok csak az érintett hozzájárulásával, vagy mérlegeléssel alátámasztott jogos érdekből, vagy közérdekből legyenek kezelhetők. Az elszámoltathatóság elvének való megfelelés érdekében, a korlátozás ilyen módon történő feloldásának dokumentálásáról, és jogszerűsége bizonyíthatóságáról a Társaságnak kell gondoskodnia.

A Társaságnak előzetesen tájékoztatnia kell az érintettet, a kérelmére történő korlátozás feloldásáról.

Adattovábbítás címzettjeinek értesítése

A Társaságoknak minden olyan címzettet tájékoztatnia kell a helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akinek az érintett adatait továbbították. Ez alól kivételt az jelent, ha a tájékoztatás lehetetlen, vagy aránytalanul nagy erőfeszítést igényel.

Adathordozhatóság

Amennyiben a Társaságok az érintett személyes adatait automatizált módon kezelik, valamint az adatkezelés jogalapja az érintett GDPR 6. cikk (1) bekezdésének a) pontja szerinti hozzájárulása vagy

a 9. cikk (2) bekezdésének a) pontja szerinti hozzájárulása vagy a 6. cikk (1) bekezdésének b) pontja szerinti vele kötött szerződés, úgy az érintett által rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban kell a rendelkezésére bocsátani.

Az adathordozhatósághoz való jog gyakorlása nem sértheti az adattörléshez való jogot leíró rendelkezésben foglaltakat, továbbá nem érintheti hátrányosan mások jogait és szabadságait.

Tiltakozáshoz való jog

Amennyiben a Társaság az érintett személyes adatait a GDPR 6. cikk (1) bekezdésének e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges vagy f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges pontja alapján kezeli, akkor az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is.

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a 6. cikk (1) bekezdésének e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges vagy f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben a Társaság 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.

Ha a személyes adatok kezelése közvetlen üzletszerzési cél 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.

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

Automatizált döntéshozatal egyedi ügyekben

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. Kivéve, ha a döntés:

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

Az a) és c) pontban említett esetekben a Társaságnak megfelelő intézkedéseket kell tennie az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy a Társaság részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

A kivételekben említett döntések nem alapulhatnak a személyes adatoknak különleges kategóriáin kivéve, ha az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult, vagy az adatkezelés jelentős közérdek miatt szükséges, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

4.1.4 Adatkezelő és adatfeldolgozó

4.1.4.1 Adatkezelő és közös adatkezelők

Főszabályként valamennyi Társaság maga felelős az általa kezelt személyes adatok védelméért, viszont, ha az adatkezelés céljait és eszközeit egy másik adatkezelővel vagy adatkezelőkkel közösen határozzák meg, akkor azzal közös adatkezelőknek minősül.

Amennyiben a Társaság és egy vagy több további önálló jogalanyisággal rendelkező adatkezelő folytat közös adatkezelést, úgy írásbeli megállapodásban kell rendezni a felelősségi köröket, és ennek a megállapodásnak az adatkezelésre vonatkozó rendelkezéseit az érintettek rendelkezésére kell bocsátani. Jogszabályi rendelkezés is meghatározhatja az egyes adatkezelők kötelezettségeit egy közös adatkezeléssel kapcsolatosan. Az érintettek jogainak akadálytalan biztosítása érdekében, az érintettek jogukat bármelyik adatkezelővel szemben gyakorolhatják.

4.1.4.2 Az adatfeldolgozó

A Társaság az egyes adatkezelési tevékenységeit kiszervezheti külső adatfeldolgozóknak, akik a Társaság megbízásából végzik az általa előre definiált adatkezelési műveleteket. Az adatfeldolgozó adatkezeléssel kapcsolatos döntéseket nem hozhat, kizárólag végrehajtja a Társasággal kötött megállapodásból fakadó kötelezettségeit. A Társaság felelőssége azt meghatározni, hogy az általa megbízott adatfeldolgozók megfelelő garanciákat nyújtsanak az adatvédelmi jogszabályoknak való megfeleléshez, és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtásához.

Az adatfeldolgozó által végzett adatkezelést olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint a Társaság kötelezettségeit és jogait meghatározó – szerződésnek kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben. A Társaságnak az adatfeldolgozói szerződésben elő kell írnia az adatfeldolgozót terhelő kötelezettségek körében, legalább az alábbiakat:

- a személyes adatokat kizárólag a Társaság írásbeli utasításai alapján kezeli, kivéve jogszabályban előírt egyedi esetekben,
- biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak,
- meghozza a megfelelő technikai és szervezési intézkedéseket, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja,
- a Társaság előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe,
- az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti a Társaságot abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében,
- segíti a Társaságot az adatkezelés biztonsága, az incidensmenedzsment, az adatvédelmi hatásvizsgálat és az előzetes konzultáció teljesítésében,
- az adatkezelési szolgáltatás nyújtásának befejezését követően a Társaság döntése alapján minden személyes adatot töröl vagy visszajuttat a Társaságnak, és törli a meglévő másolatokat, kivéve, ha jogszabály másként rendelkezik,
- a Társaság rendelkezésére bocsát minden olyan információt, amely az adatfeldolgozó igénybevételével kapcsolatos kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti a Társaság által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is. Ezen információknak a Társaság rendelkezésére bocsátásával kapcsolatosan az adatfeldolgozónak haladéktalanul tájékoztatnia kell a Társaságot, ha úgy véli, hogy annak valamely utasítása adatvédelmi jogszabályt sért.

A Társaságnak az adatfeldolgozóval kötött adatfeldolgozói szerződésben ki kell térnie továbbá arra, hogy amennyiben az adatfeldolgozó, további adatfeldolgozót vesz igénybe, úgy ugyanazokat az adatvédelmi kötelezettségeket kell meghatározni a további adatfeldolgozóra, mint amelyeket az adatkezelési szerződésben meghatározott a Társaság az adatfeldolgozó számára.

4.2 Általános feladatok, felelőségek és hatáskörök

Az adott Társaság vezető tisztségviselője

Gondoskodnia kell a Társaság adatvédelmi stratégiájának jóváhagyásáról.

A biztonsági vezető tájékoztatása alapján, az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények-, az esetlegesen feltárt adatbiztonsági hiányosságok megszüntetésére intézkednie kell.

Adatkezelő szervezeti egység vezetője

Az előírásoktól eltérő adatkezelési gyakorlatra vonatkozó értesítés esetén gondoskodnia kell a szabályszerű állapot helyreállításáról.

Amennyiben a Társaságon belüli Adatkezelő szervezeti egységek együttesen folytatnak közös adatkezelést, akkor az adatkezeléssel járó szakmai folyamatot leíró szabályzatban kell rendezniük az adatkezelés kapcsán felmerült kötelezettségeiket, különös tekintettel az érintettek tájékoztatására és jogaik gyakorlásának biztosítására.

Az adatkezelő szervezeti egység vezetője a biztonsági vezető szakmai javaslata alapján dönt a biztonsági vezető ellenőrzése során tett megállapítások és javaslatok foganatosítása tekintetében. Ha az adatkezelő szervezeti egység vezetője nem veszi figyelembe a szakmai javaslatot, akkor írásban köteles megindokolni a szakmai javaslatban megfogalmazottak figyelmen kívül hagyását és azt, hogy a döntése során milyen módon juttatja érvényre az adatvédelmi elveket és ezen utasítás előírásait.

Folyamatos változásjelentési kötelezettséggel tartozik a biztonsági vezető részére. ha a szervezeti egység adatkezelésében változás áll be, azt azonnal közli a biztonsági vezetővel.

A személyes adatokat érintő incidens esetén azonnal tájékoztatja a Magyar Vagon Befektetési Vagyonkezelő Zrt. vezető tisztségviselőjét és jogi vezetőjét, valamint a biztonsági vezetőt. Részt vesz az incidens kivizsgálásában, a szükséges dokumentumok létrehozásában, kitöltésében.

Hatóság megkeresése esetén részt vesz a tények kiderítésében, az információk összegyűjtésében és a választervezet elkészítésében.

Biztonsági vezető

Tájékoztatnia kell a Társaságok vezető tisztségviselőit az adatkezelésre irányuló ellenőrzés során feltárt hiányosságokról vagy jogszabálysértő körülményekről.

A biztonsági vezető a csoportszintű adatvédelmi szabályzatot, valamint a Társaságok saját adatvédelmi szabályzatát előkészíti és szükség szerinti módosítására javaslatot tesz – csoportszintű szabályzat esetén a Magyar Vagon Befektetési Vagyonkezelő Zrt. vezető tisztségviselője, az érintett Társaság esetén annak vezető tisztségviselője részére.

Adatvédelmi vizsgálatot folytathat le.

Feladatai ellátása során jogosult teljes mértékben betekinteni a Társaságoknál végzett összes adatkezelés és adatfeldolgozás dokumentumaiba, és jogosult teljes körű tájékoztatást kapni a vizsgált adatkezelésekről. Minden olyan adatkezelést megismerhet, amely személyes adatokkal összefügg, és minden helyiségbe beléphet, ahol adatkezelés folyik.

Írásbeli tájékoztatást és szakmai tanácsot, állásfoglalást kell adnia az adatkezelő és az adatkezelést végző alkalmazottak részére.

A biztonsági vezető ellenőrzi a GDPR-nek, 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 résztvevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is.

A biztonsági vezető értesíti az ellenőrizni kívánt szervezeti egység vezetőjét az auditról/ellenőrzésről. Az ellenőrzés során tett észrevételeket és javaslatokat a biztonsági vezető írásban megküldi az adott szervezeti egység vezetőjének.

Az adatkezelő szervezeti egység vezetője a biztonsági vezető szakmai javaslata alapján dönt az ellenőrzés során tett megállapítások és javaslatok foganatosítása tekintetében. Ha az adatkezelő szervezeti egység vezetője nem veszi figyelembe a szakmai javaslatot, akkor írásban köteles megindokolni a szakmai javaslatban megfogalmazottak figyelmen kívül hagyását és azt, hogy a döntése során milyen módon juttatja érvényre az adatvédelmi elveket és ezen utasítás előírásait. A szervezeti egység vezető szakmai javaslat ellenében meghozott döntése nem lehet ezen utasításba foglaltakkal ellentétes. Amennyiben a szervezeti egység vezetője a biztonsági vezető szakmai javaslata ellenében dönt, úgy az írásbeli indoklását a biztonsági vezető köteles felülvizsgálni. Amennyiben a biztonsági vezető úgy ítéli meg, hogy a döntéshozó döntése nem felel meg az adatvédelmi elveknek és ezen utasítás előírásainak, erről feljegyzést készít az érintett Társaság vezető tisztségviselője részére.

Támogatja az érintett szervezeti egységeket az adatvédelmi szabályok beépítésében az egyes utasításokba/szabályzatokba, az adatkezelési tájékoztatók elkészítésében, az érdekmérlegelési tesztek elkészítésében, a Hatóság megkeresései megválaszolásának előkészítésében, az új informatikailag támogatott adatkezelések informatikai rendszereinek hatásvizsgálatának elkészítésében.

A Humánerőforrás igazgatóság által az adatkezelők részére szervezett oktatáshoz és éves továbbképzéshez kérés esetén szakmai támogatást nyújt.

Munkáltatói jogkörgyakorló minőségében felügyelni kell az Információvédelmi szakértő munkavégzését.

Éves adatbiztonsági ellenőrzési tervet kell elfogadnia, vagy az éves biztonsági ellenőrzési tervben adatbiztonsági ellenőrzéseket kell beterveznie.

Információbiztonsági szakértő

Éves ellenőrzési tervet kell készítenie, továbbá a Társaság rendszereiben és számítógépes alkalmazásaiban ellenőriznie kell az adatbiztonsági követelmények megvalósulását.

Feladatai ellátása során jogosult teljes mértékben betekinteni a Társaságnál végzett összes adatkezelés és adatfeldolgozás dokumentumaiba, és jogosult teljes körű tájékoztatást kapni a vizsgált adatkezelésekről. Minden olyan adatkezelést megismerhet, amely személyes adatokkal összefügg, és minden helyiségbe beléphet, ahol adatkezelés folyik.

4.3 Feladatok és felelősségek az adatkezelés megkezdése előtt

Az utasítás jelen szakasza 4.3-as ponttól a 4.5-ös pontig bezáróan az adatkezeléssel járó szakmai folyamatért felelős, adatkezelő szervezeti egység és egyéb résztvevők feladat és felelősségét határozza meg az adatkezelés egyes szakaszaiban. Az előbbieken jelzett szakaszokban helyenként visszautalás történik az általános leírást tartalmazó 4.1-es pontra, ahol bár adatkezelőként az adott Társaság került megjelölésre, a feladatok és felelősségek továbbra is az adott szakmai folyamatért felelős Adatkezelő szervezeti egységet terhelik.

4.3.1 Az Adatkezelő szervezeti egység feladata

Az adott szervezeti egységnél zajló egyes adatkezeléssel járó szakmai folyamatok adatvédelmi megfelelése, az ilyen folyamatok kialakítása, az elkészült folyamatnak és folyamatábrának biztonsági vezetővel történő dokumentált megismertetése az Adatkezelő szervezeti egység vezetőjének felelősségi körébe tartozik.

Az Adatkezelő szervezeti egységnek az adatkezeléssel járó folyamat megtervezésének kezdetén be kell vonnia a biztonsági vezetőt, hogy szakmai segítséget nyújtson a megfeleléshez.

Az Adatkezelő szervezeti egységnek a biztonsági vezető közreműködésével úgy kell kialakítania az adatkezeléssel járó tevékenységét, hogy az megfeleljen a hatályos jogszabályoknak, dokumentált legyen, biztosítsa az érintettek jogainak gyakorlását, és szavatolja a személyes adatok biztonságát.

4.3.1.1 Hatásvizsgálat

Amennyiben az Adatkezelő szervezeti egység a személyes adatok kezelésével járó tevékenység tervezésekor úgy ítéli meg, hogy az az érintettek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal jár, akkor a tervezési folyamat részeként adatvédelmi hatásvizsgálatot kell folytatnia. Az adatvédelmi hatásvizsgálat lefolytatásában az Adatkezelő szervezeti egységnek a biztonsági vezető szakmai segítségét kell kérnie.

Az adatvédelmi hatásvizsgálat elvégzése minden esetben kötelező különösen, ha:

- a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelésére kerül sor, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek,
- a személyes adatok különleges kategóriái, vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és büncselekményekre vonatkozó személyes adatok nagy számban történő kezelésére kerül sor,
- a nyilvános helyek nagymértékű, módszeres megfigyelésére kerül sor, vagy
- a tervezett adatkezelési művelet szerepel a Hatóság által közzétett, kötelező eseteket tartalmazó listán.

Amennyiben az adatkezeléssel járó tevékenység nem esik a fent említett kategóriákba, a hatásvizsgálat szükségességének eldöntéséhez az alábbi kockázati tényezők meglétét kell mérlegelni:

- Értékelés vagy pontozás, ideértve a profilalkotást és az előrejelzést is, különösen az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján.
- Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: adatkezelés, amelynek célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala.
- Módszeres megfigyelés: érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztül adatgyűjtés vagy a nyilvános helyek nagymértékű, módszeres megfigyelése.
- Különleges adatok vagy fokozottan személyes jellegű adatok kezelése.
- Nagy számban kezelt adatok:
 - = az érintettek száma konkrét számadatként vagy a lakosság arányában
 - = a kezelt adatok mennyisége vagy adatfajták köre
 - = az adatkezelési tevékenység időtartama vagy állandó jellege
 - = az adatkezelési tevékenység földrajzi kiterjedése.
- Adatkészletek egymással való megfeleltetése vagy összevonása például két vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett ésszerű elvárásait meghaladó módon.
- Kiszolgáltatókban lévő érintettekkel kapcsolatos adatok
 - = gyermekek
 - = munkavállalók
 - = lakosság különleges védelmet igénylő rétegei vagy
 - = minden olyan esetben, amikor az érintett és az adatkezelő közötti kapcsolatban egyenlőtlen helyzet alakul ki.
- Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: például az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében.
- Azok az esetek, amikor az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek. Ide tartoznak az érintettek számára szolgáltatás igénybevételének vagy szerződéskötésnek a lehetővé tételére, módosítására vagy elutasítására irányuló adatkezelési műveletek.

Minél több az előzőekben felsorolt szempontnak felel meg az adatkezelés, annál nagyobb a valószínűsége annak, hogy az magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

Amennyiben az Adatkezelő szervezeti egység, a fent említett körülmények vizsgálata alapján, és a biztonsági vezető állásfoglalása ellenére a hatásvizsgálat lefolytatását mellőzi, úgy dokumentáltan alá kell támasztania az adatvédelmi hatásvizsgálat mellőzésének okait.

Az adatvédelmi hatásvizsgálat elvégzése nem kötelező, ha:

- ha az adatkezelés valószínűsíthetően nem jár magas kockázattal a természetes személyek jogaira és szabadságaira nézve,
- ha az adatkezelés a jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít egy olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat, ilyen esetekben felhasználhatók a Társaság által korábban elvégzett, hasonló adatkezelés adatvédelmi hatásvizsgálatának eredményei,
- ha az adatkezelési műveleteket a Hatóság 2018. május előtt már ellenőrizte és az adatkezelés feltételei azóta nem változtak meg,
- ha az adatkezelés jogi kötelezettség teljesítésén- vagy közérdeken-, vagy közhatalmi jogosítvány gyakorlásán alapszik; és jogszabály szabályozza az adott adatkezelési műveletet; és ezen jogszabály alapján végzett adatkezelésre már készült adatvédelmi hatásvizsgálat; feltéve, hogy a jogszabályban nincs kifejezetten kimondva, hogy minden esetben hatásvizsgálatot kell végezni,
- ha az adatkezelés szerepel a Hatóság által összeállított, a nem kötelező adatkezelési műveletek jegyzékében, amelyekre tekintettel nem kötelező hatásvizsgálatot készíteni.

Az adatvédelmi hatásvizsgálatot rendszeres időközönként felül kell vizsgálnia az Adatkezelő szervezeti egységnek. A felülvizsgálatot legalább két évente el kell végezni. A felülvizsgálatot haladéktalanul le kell folytatni, amennyiben az adatkezelés lényeges körülményei:

- a hatókör,
- a cél,
- a gyűjtött személyes adatok köre,
- az adatkezelők vagy címzettek kiléte,
- az adatmegőrzési időszak,
- a technikai és szervezési intézkedések,
- az alkalmazott technológia változnak.

Érintettek véleményének kikérése

Az Adatkezelő szervezeti egységnek ki kell kérnie az érintettek vagy képviselőik véleményét a tervezett adatkezelésről. Mellőzhető az érintettek véleményének kikérése, ha az által a Társaság üzleti tervének titkossága sérülne, illetve aránytalan vagy kivitelezhetetlen lenne ez az intézkedés. Amennyiben az Adatkezelő szervezeti egység úgy dönt, hogy nem kéri ki az érintettek véleményét, akkor nemleges döntését dokumentumokkal kell alátámasztania.

Hatásvizsgálat lefolytatása, és az előzetes konzultáció

Az Adatkezelő szervezeti egységnek az 1. számú melléklet alapján kell elvégeznie az adatvédelmi hatásvizsgálatot. Amennyiben a Hatóság honlapjáról letölthető adatvédelmi hatásvizsgálat szoftver rendelkezésre áll az Adatkezelő szervezeti egység részére, úgy az adatvédelmi hatásvizsgálatot annak segítségével kell elvégezni.

Amennyiben a hatásvizsgálat eredménye alapján, a kockázatmentes intézkedések ellenére, az adatkezelés továbbra is valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira, úgy az Adatkezelő szervezeti egység a biztonsági vezető szakmai támogatása mellett előzetes konzultációt kell, hogy kezdeményezzen a Hatósággal.

Az előzetes konzultáció során az Adatkezelő szervezeti egységnek tájékoztatást kell adnia a Hatóságnak:

- az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiből, különösen vállalkozáscsoporton belüli adatkezelés esetén;
- a tervezett adatkezelés céljairól és módjairól;
- az érintettek a GDPR értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;
- az adatvédelmi feladatok ellátásával megbízott munkavállaló elérhetőségeiről;
- az adatvédelmi hatásvizsgálatról;
- a felügyeleti hatóság által kért minden egyéb információról.

Az Adatkezelő szervezeti egységnek az adatkezeléssel járó szakmai folyamat megtervezése során figyelemmel kell lennie arra, hogy a Hatóság az előzetes konzultáció iránti megkeresésre a kézhezvételétől számított nyolc héten belül ad írásban tanácsot, illetve ez a határidő hat héttel meghosszabbítható. Figyelemmel kell lennie továbbá arra is, hogy az említett időtartamok felfüggeszthetők arra az időtartamra, amíg a felügyeleti hatóság nem jut hozzá azokhoz az információkhoz, amelyeket a konzultáció céljából kért.

4.3.1.2 Jogalap

Az Adatkezelő szervezeti egységnek az adatkezelés megkezdését megelőzően meg kell határoznia az adatkezelés jogalapját figyelemmel a 4.1.2. pontban foglaltakra.

4.3.1.3 Érdemérlegelési teszt

Amennyiben a jogalap meghatározása a GDPR 6. cikk (1) bekezdés f) pontja, azaz a Társaság jogos érdeke, úgy az Adatkezelő szervezeti egységnek érdemérlegelési tesztet kell végeznie (2. sz. melléklet szerint).

Érdemérlegelési teszt elkészítésének folyamata:

1. lépés: a Társaság a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.
2. lépés: a Társaság a jogos érdekét a lehető legpontosabban meghatározza.
3. lépés: a Társaság meghatározza, hogy mi az adatkezelés célja, milyen személyes adatok, milyen időtartammal történő adatkezelését igényli a jogos érdek.
4. lépés: a Társaság meghatározza, hogy az érintetteknek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (pl. azok a szempontok, amelyeket az érintettek érvként felhozhatnak az adatkezeléssel szemben).
5. lépés: a Társaság elvégzi jogos érdekeinek és az érintettek érdekeinek, alapjogainak súlyozását és ez alapján megállapítja, hogy a személyes adat kezelhető-e. A Társaság meghatározza, hogy miért korlátozza arányosan a Társaság jogos érdeke – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott érdekelti jogokat, várakozásokat.
6. lépés: a Társaság meghatározza, mely garanciák biztosíthatják az adatkezelés szükségességét-arányosságát (természetesen más garanciális intézkedések is alkalmazhatók).
7. lépés: Érdemérlegelés eredménye és annak dokumentálása.

4.3.1.4 Adatbiztonság

Az Adatkezelő szervezeti egység felelőssége, hogy az adatkezelés megtervezése folyamán

- a tudomány és technológia állása és a megvalósítás költségei, továbbá
- az adatkezelés jellege, hatóköre, körülményei és céljai, valamint

- a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével

megfelelő technikai és szervezési intézkedéseket hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Ezen intézkedések, többek között

- a személyes adatok álnevesítése és titkosítása,
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének biztosítása,
- fizikai vagy műszaki incidens esetén az arra való képesség, hogy a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állása kellő időben visszaállítható legyen,
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárás kialakítása.

Miután az adatkezelés megtervezésének folyamata abba a szakaszba ért, hogy a jogszerűség-, tisztességes eljárás- és átláthatóság-, adattakarékosság-, pontosság-, korlátozott tárolhatóság-, elvének érvényesülése biztosított, – tehát az adatkezelő a biztonsági vezető bevonásával megtervezte az adatkezeléssel járó tevékenységét és meghatározta a kezelni kívánt adatok körét – az integritás- és bizalmas jelleg- elvének való megfelelés elősegítése érdekében az adatkezelő bevonja a Biztonsági szervezet Információvédelemi szakértőjét (amennyiben az adott Társaság mindenkor hatályos Szervezeti és Működési Szabályzata alapján a Társaságnál van ilyen beosztású munkavállaló).

Technikai elvárások a tervezés során:

- A személyes adatokat tároló számítógépes adathordozóját teljes kapacitásában titkosítani kell.
- Külön védelmi intézkedéseket kell tenni, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.
- A szerver számítógépek és a munkaállomások között személyes adatokat védetten (titkosítva) kell továbbítani.
- A Társaság alkalmazottainak és ügyfeleinek személyes adatait tartalmazó adatbázisokat a Társaság Informatikai Biztonsági Szabályzatában (a továbbiakban: IBSZ) definiált ún. **bizalmasság és sértetlenség szerinti „fokozott” biztonsági osztálynak megfelelő** védelemben kell részesíteni.

A rendszerekben a felhasználói jogosultságok korlátozásával biztosítani kell, hogy a hozzáférésre jogosultak kizárólag a munkájukhoz feltétlenül szükséges személyes adatokat ismerhessék csak meg.

A rendszereket a Társaság IBSZ-ében foglalt előírások szerint kell kifejleszteni, az ott előírt biztonsági dokumentumok elkészültét követően szabad használatba venni és üzemeltetni.

- Személyes adatot tartalmazó valamennyi dokumentumot ”Nem nyilvános!” kezelési jelzéssel kell ellátni. A jelzést a dokumentum (pl.: munkaszerződés, fizetési besorolás, a személyes adatokat tartalmazó adatbázis felhasználásával készített Excel-táblázat, kedvezményes utazásra jogosító kártya igénylőlapja) minden egyes lapjának fejrészában a készítőnek fel kell tüntetnie. E minősítési jelzés mellett az ilyen dokumentumot iktatási számmal is el kell látni, kivéve, ha azon más, a dokumentum egyedi azonosítására alkalmas jelzés található.
- Ha a személyes adat számítógépes képernyőn kerül megjelenítésre, akkor a képernyő felső részén meg kell jeleníteni a ”Nem nyilvános!” kezelési jelzést. A monitort úgy kell elhelyezni, hogy a többszemélyes irodában dolgozók, és az irodába belépő más személyek illetéktelenül ne ismerhessék meg a képernyőn megjelenő személyes adatokat.
- Személyes adat másolása az elektronikus adathordozóra kizárólag titkosított módon történhet. A „Nem nyilvános” jelzéssel ellátott dokumentumokat, és a személyes adatokat tartalmazó adathordozókat zárral ellátott fa szekrényben, vagy lemezszekrényben kell tárolni. A ronggott és a munkapéldányokat megsemmisítésükig ugyanezen szabályok szerint kell tárolni.

4.3.1.5 Érintetti jogok és az érintett tájékoztatása

Érintetti jogok

Az Adatkezelő szervezeti egységnek úgy kell kialakítania az adatkezeléssel járó szakmai folyamatait, hogy a 4.1.3. pontban foglalt érintetti jogok gyakorolhatóságát biztosítani tudja.

Adatkezelési tájékoztató elkészítése

A Társaságot terhelő előzetes tájékoztatási kötelezettséggel kapcsolatos feladatokat az adatkezelő szervezeti egység látja el. Ennek keretében az adatkezelő szervezeti egység az adatkezelési folyamat tervezését követően a 4. számú mellékletben foglalt minta alapján – a biztonsági vezető közreműködésével – elkészíti az adatkezelési tájékoztatót. A 4. számú melléklet szerinti adatkezelési tájékoztató minta szövegétől az adatkezelési folyamat jellegére és az adatkezelés körülményeire tekintettel el lehet térni.

Az adatkezelő szervezeti egység gondoskodik az adatkezelési tájékoztatónak az érintettekkel történő – a jelen utasításban foglaltak szerinti – megismertetéséről. Amennyiben a jelen utasítás szerint az adatkezelési tájékoztatót a Társaság honlapján közzé kell tenni, úgy a közzétételről a biztonsági vezető gondoskodik.

Az adatkezelési tájékoztató közlésére vonatkozó szabályok:

Az adatkezelési tájékoztató közlésének kötelezettségére vonatkozó szabályokat – az adatkezelési folyamat tekintetében irányadó szabályzatban – úgy kell meghatározni, hogy a Társaság igazolni tudja az adatkezelésre vonatkozó információk rendelkezésre bocsátására vonatkozó kötelezettségének teljesítését. A tájékoztatási kötelezettség teljesítéséhez az adatkezelésre irányadó adatkezelési tájékoztató érintett részére történő megismerhetővé tételre van szükség. Amennyiben az adatkezelés jogszerűségét az érintett hozzájárulása biztosítja, az adatkezelési tájékoztatót a hozzájáruló nyilatkozat megtételét megelőzően meg kell ismertetni az érintettel. Az adatkezelési tájékoztató megismeréséről az érintettet minden esetben nyilatkoztatni kell.

Ha az adatkezelő szervezeti egység a személyes adatok gyűjtésére egyedi elektronikus felületet alkalmaz, úgy az elektronikus felületet úgy kell kialakítani, hogy az érintett az adatkezelési tájékoztatót az adatkezelés megkezdését megelőzően megismerhesse. Amennyiben az elektronikus felület alkalmas arra, azon folyamatosan elérhetővé kell tenni az elektronikus felületen végzett adatkezelésre vonatkozó adatkezelési tájékoztatót. A személyes adatok gyűjtésére alkalmazott egyedi elektronikus felületet úgy kell kialakítani, hogy amennyiben az adatkezelési tájékoztató az adatkezelés során megváltozik, úgy az érintett e változásról tájékoztatható legyen.

Ha az adatkezelés keretében az adatkezelő szervezeti egység a személyes adatokat elektronikus úton gyűjti, de az adatkezelő szervezeti egység nem rendelkezik a személyes adatok gyűjtéséhez alkalmazott egyedi elektronikus felülettel (pl. az érintett által küldött e-mail alapján kezdődik meg az adatkezelés), úgy az adatkezelési tájékoztató elérhetőségéről az érintettet tájékoztatni kell az adatkezelési folyamattal összefüggésben közzétett információk keretében. Az adatkezelő szervezeti egységeknek törekedniük kell arra, hogy az egyes adatgyűjtéssel járó folyamatok keretében elektronikus vagy papír alapon előterjeszhető formanyomtatványt alkalmazzanak.

Amennyiben az adatkezelés keretében az adatkezelő szervezeti egység a személyes adatokat papír alapú dokumentum keretében gyűjti és az adatkezelés körülményeire tekintettel az – igazolható módon megtett – előzetes tájékoztatás nem valósítható meg másképpen, a papír alapú dokumentum bármelyik oldalán vagy az ahhoz csatolt dokumentumon fel kell tüntetni legalább az adatkezelési tájékoztató – GDPR-ban foglalt minimum követelményeknek megfelelő – kivonatát, amelyen az érintettet tájékoztatni kell az adatkezelési tájékoztató bővített változatának elérhetőségéről.

Amennyiben az adatkezelési tájékoztató az adatkezelési folyamat során megváltozik és az adatkezelő szervezeti egység rendelkezik az érintett elektronikus elérhetőségével, úgy az érintettet elektronikus úton tájékoztatni kell az adatkezelési tájékoztató megváltozásáról.

A Társaság az általa foglalkoztatott személyekkel az adatkezelési tájékoztatót az adatkezelési tájékoztatót tartalmazó szabályzatnak közzétételével vagy az adatkezelési tájékoztató munkáltatói jogkör gyakorló részére elektronikus úton történő megküldésével közli, mindezt azzal, hogy a munkáltatói jogkörgyakorlója köteles valamennyi, az irányítása alatt lévő érintett részére elektronikus úton vagy a helyben szokásos módon (pl. parancskönyvi rendelkezés kiadásával) megküldeni az adatkezelési tájékoztatót.

Az adatkezelési tájékoztató közzétételére vonatkozó kötelezettségek:

Azt az adatkezelési tájékoztatót, amely olyan adatkezelésre vonatkozik, amelyben a Társaság olyan érintett személyes adatát is kezeli, aki nem áll foglalkoztatásra irányuló jogviszonyban a Társasággal, a Társaság honlapján közzé kell tenni és annak elérhetőségét folyamatosan biztosítani kell. A közzétételről – az adatkezelési tájékoztató biztonsági vezető által történő megküldése mellett – a Titkárság szervezeti egység gondoskodik (amennyiben az adott Társaságnál nincs Titkárság szervezeti egység, úgy a Társaság honlapjának kezelésével megbízott szervezeti egység).

A Társaság által foglalkoztatott személyek, mint érintettek részére az adatkezelési tájékoztatót

- a) az elektronikus elérhetőséggel rendelkező érintettek részére a „Közös meghajtón”,
- b) az elektronikus elérhetőséggel nem rendelkező érintettek részére a helyben szokásos módon kell közzé tenni és biztosítani annak elérhetőségét.

Helyben szokásos módon történő közzététel teljesíthető azzal, hogy a munkavállaló érintett tájékoztatásra kerül arról, hogy mely elektronikus elérhetőséggel rendelkező munkavállalótól kérheti az adatkezelési tájékoztató rendelkezésre bocsátását papír alapon is. Erről a munkavállaló munkáltatói jogkörgyakorló vezetője gondoskodik.

4.3.1.6 Adatkezelés nyilvántartása

Az Adatkezelő szervezeti egység az adatkezelésről nyilvántartást vezet. Ebben nyilvántartja az általa végzett adatkezelési folyamatok tekintetében alkalmazott valamennyi – hatályos és hatályát veszített – adatkezelési tájékoztatót. Az adatkezelést bejelenti a biztonsági vezető részére. A biztonsági vezető vezeti a Társasági szintű Belső adatvédelmi nyilvántartást.

4.3.1.6.1 Az adatkezelő szervezeti egység feladata

Az Adatkezelő szervezeti egység az adatkezeléssel járó tevékenységeiről a 3. sz. mellékletben előírtak szerint kitölti az „Adatlap adatkezelési tevékenységek nyilvántartásához” adatlapot. Az Adatkezelő szervezeti egységnek az adatkezelés megkezdése előtt a 3. sz. mellékletet meg kell küldenie a biztonsági vezető részére. A biztonsági vezető felveszi a Belső adatvédelmi nyilvántartásba.

4.3.1.6.2 A biztonsági vezető feladata

Az adatkezeléssel járó szakmai folyamatok megtervezésében történő bevonását követően, dokumentált szakmai tanácsot kell adnia az Adatkezelő szervezeti egység részére.

A biztonsági vezetőnek szakmai tanácsot kell adnia az adatvédelmi hatásvizsgálat lefolytatásának szükségességére, illetve az Adatkezelő szervezeti egység által előkészített hatásvizsgálatot értékelnie kell, valamint az elkészített hatásvizsgálatot véleményeznie kell.

Amennyiben a hatásvizsgálat eredménye alapján, a kockázatmérséklő intézkedések ellenére, az adatkezelés továbbra is valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira, úgy az Adatkezelő szervezeti egység kezdeményezésére indított előzetes konzultációhoz szakmai segítséget kell nyújtania.

Az érdekmérlegelési tesztbe történő bevonása esetén, szakmai tanácsot kell adnia az Adatkezelő szervezeti egység részére.

A szakmai tanácsadásnak ki kell terjednie az érintetti jogok biztosításának rendjére, illetve az érintett előzetes tájékoztatására, azaz az adatvédelmi tájékoztatók összeállítására is.

A biztonsági vezető vezeti a Társasági szintű összesített Belső adatvédelmi nyilvántartást. A Belső adatvédelmi nyilvántartás adattartalmát az Adatkezelő szervezeti egységektől megkapott „Adatlap adatkezelési tevékenységek nyilvántartásához” adatlapok (3. sz. melléklet) képzik. A belső adatvédelmi nyilvántartásban az egyes adatkezeléseket egyedi azonosítóval kell ellátni, amelyet a biztonsági vezetőnek kell vezetnie.

4.3.2 A Biztonsági szervezet információbiztonsági szakértőjének feladata

A Biztonsági szervezet támogatást nyújt az adatkezelők részére az adatkezelési tevékenység adatbiztonsági követelményeinek kialakításában.

Az adatvédelmi hatásvizsgálat lefolytatása során a felmerülő adatbiztonsági kockázatok feltárása, mérséklése érdekében az Adatkezelő szervezeti egység megkeresése esetén szakmai segítséget kell, hogy nyújtson.

Az adatkezelési tájékoztató elkészítése során az Adatkezelő szervezeti egység megkeresése esetén az „Adatbiztonsági intézkedésekről szóló tájékoztatás” rész kitöltéséhez szakmai segítséget nyújt.

4.4 Feladatok és felelősségek a személyes adatok kezelése során

A személyes adatok kezelése során a kialakított nyilvántartásokat naprakészen kell tartani, a bekövetkezett incidenseket kezelni kell, a hatásvizsgálatokat felül kell vizsgálni, a személyes adatok kezelése során az érintettek részére jogaik gyakorlását lehetővé kell tenni.

A Társaságok minden munkavállalója és a Társaságokkal szerződésben álló szervezetek minden munkatársa köteles az általa megismert, vagy számára bejelentett adatvédelmi incidenst – a lehető leghamarabb, de legkésőbb annak tudomására jutásától számított 4 órán belül – jelenteni a biztonsági vezetőnek telefonon és részletesen leírva az adatvédelem@mavag.hu e-mail elérhetőségen.

4.4.1 Az Adatkezelő szervezeti egység feladata

4.4.1.1 Adatkezeléssel járó szakmai folyamat módosítása, időszakos felülvizsgálata

Amennyiben a személyes adatkezeléssel járó szakmai folyamatban olyan lényeges változás következik be, amely a személyes adatok kezelésére is hatással van, úgy az új szakmai folyamat tervezésénél ismét figyelembe kell venni jelen utasítás 4.1., 4.2. és 4.3. pontjában foglaltakat. Ha az adatkezeléssel járó szakmai folyamatban nem következik be változás, akkor is két évente felül kell vizsgálni az adatkezeléssel járó szakmai folyamatokat leíró utasításokat. Továbbá, adatvédelmi incidens bekövetkezése-, valamint a személyes adatkezelést érintő jogszabályi változás esetén is felül kell vizsgálni az adatkezeléssel járó szakmai folyamatot, illetve az azt leíró utasításokat.

4.4.1.2 Adatvédelmi hatásvizsgálat felülvizsgálata

Az adatvédelmi hatásvizsgálatot felül kell vizsgálni és újra kell értékelni, valahányszor csak olyan változás következik be az adatkezelésben vagy a rá ható külső körülményekben, amely magas kockázati szintet eredményez.

Ezen túlmenően az Adatkezelő szervezeti egységnek két évente felül kell vizsgálnia és újra kell értékelnie a hatásvizsgálatot, függetlenül attól, hogy az adatkezelés körülményeiben történt-e változás, és annak eredményeként az adatvédelmi hatásvizsgálatot aktualizálni kell.

Az Adatkezelő szervezeti egységnek a hatásvizsgálat felülvizsgálata és újraértékelése során a 4.3.1.1. pont vonatkozó rendelkezéseire kell figyelemmel lennie.

4.4.1.3 Érintetti jogok biztosításával összefüggő feladatok

Az adatkezelési tájékoztatókon szerepeltetett elérhetőségeken keresztül, az érintettektől érkező megkereséseket az Adatkezelő szervezeti egységnek kell kezelnie, a tervezés folyamán a 4.3.1.5-ös pont szerint kialakított belső folyamat szerint. Az Adatkezelő szervezeti egység a biztonsági vezető szakmai segítségét kérheti a megkeresések teljesítése érdekében.

Amennyiben az érintett vitatja az Adatkezelő szervezeti egység eljárásának jogszerűségét, úgy az Adatkezelő szervezeti egységnek felül kell vizsgálnia a vitatott eljárását a jelen utasítás 4.3. pont szerint. Amennyiben nem ért egyet az érintett az Adatkezelő szervezeti egység észrevételével, úgy az Adatkezelő szervezeti egységnek az érintettet a biztonsági vezetőhöz kell irányítania.

Az érintett részéről érkezett megkereséseket az Adatkezelő szervezeti egységnek a 4.1.3. pontban meghatározott határidők betartása mellett kell teljesítenie.

4.4.1.4 Incidenskezelés

Az Adatkezelő szervezeti egységnek a biztonsági vezető szakmai támogatása mellett össze kell gyűjtenie mindazokat az információkat, ami alapján a biztonsági vezető ki tudja tölteni az 5. sz. mellékletet, az Adatvédelmi Incidens nyilvántartást.

A biztonsági vezető számára megküldött bejelentésnek tartalmaznia kell legalább:

- az incidensről való tudomásszerzés időpontját,
- az incidens jellegét, tárgyát, rövid leírását,
- az incidenssel kapcsolatban rendelkezésre álló valamennyi információt.

Amennyiben az adatvédelmi incidens adatbiztonsági vagy informatikai szakmai kérdést érint, úgy az Adatkezelő szervezeti egység a Biztonsági szervezet információbiztonsági szakértője vagy az Informatika szervezet szakmai segítségét kérheti.

Az így összegyűjtött információk birtokában a biztonsági vezető szakmai támogatása mellett, az Adatkezelő szervezeti egység el kell, hogy végezze az incidens hatásának mérlegelését, hogy az valószínűsíthetően kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve.

Amennyiben a mérlegelés eredményeként az incidens kockázattal jár a természetes személyek jogaira és szabadságára nézve, az Adatkezelő szervezeti egység a biztonsági vezetőn keresztül be kell, hogy jelentse a Hatóság részére. Az Adatkezelő szervezeti egységnek a lehető leghamarabb, de legkésőbb annak tudomására jutásától számított 4 órán belül jelenteni kell a Magyar Vagon Befektetési Vagyonkezelő Zrt. vezető tisztségviselőjének és jogi vezetőjének e-mailben, valamint a biztonsági vezetőnek az adatvedelem@mavag.hu e-mail elérhetőségen. A biztonsági vezetőnek lehetőség szerint az észlelésétől számított 72 órán belül be kell jelentenie az incidenst a Hatóság részére. Ha a Hatóságnak történő bejelentés alkalmával, nem lehetséges az információkat egyidejűleg közölni, akkor azok további indokolatlan késedelem nélkül, később részletekben kell közölni, amelyhez mellékelni kell a késedelem igazolására szolgáló indokokat is.

Amennyiben a mérlegelés eredményeként az incidens magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, a biztonsági vezető szakmai támogatása mellett, a hatósági bejelentésen túl, köteles az incidenssel érintetteket tájékoztatni az alábbiakról:

- a biztonsági vezető vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetősége,
- az adatvédelmi incidensből eredő, valószínűsíthető következmények,
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Nem kell az érintetteket tájékoztatni:

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

4.4.2 A biztonsági vezető feladatai

A biztonsági vezetőnek az Adatkezelő szervezeti egység kérésére szakmai támogatást kell nyújtania az adatkezeléssel járó szakmai folyamatok felülvizsgálatához, adatvédelmi hatásvizsgálat felülvizsgálatához, és az érintetti jogokkal kapcsolatos igények teljesítéséhez.

A biztonsági vezetőnek kell irányítania a Társaság adatkezelési tevékenysége során bekövetkezett adatvédelmi incidensek kivizsgálását, ellenőriznie kell az Adatkezelő által végzett incidenskezelést.

A biztonsági vezetőnek a hozzá megküldött adatvédelmi incidensekről nyilvántartást kell vezetnie az 5. sz. melléklet szerinti adattartalommal.

A biztonsági vezetőnek szakmai támogatást kell nyújtania az adatvédelmi incidensek kivizsgálásában, különös tekintettel az incidens hatásának mérlegelésében. Amennyiben a mérlegelés eredményeként az incidens kockázattal jár a természetes személyek jogaira és szabadságára nézve, az Adatkezelő szervezeti egység által összegyűjtött információkat be kell jelentenie a Hatóságnak az erre a célra kialakított online felületen keresztül.

Az incidenst lehetőség szerint az észlelésétől számított 72 órán belül kell a Hatóságnak jelenteni. Ha a Hatóságnak történő bejelentés alkalmával, nem lehetséges az információkat egyidejűleg közölni, akkor azok további indokolatlan késedelem nélkül, később részletekben kell közölni, amelyhez mellékelni kell a késedelem igazolására szolgáló indokokat is. Amennyiben a mérlegelés eredményeként az incidens magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, a biztonsági vezető köteles szakmai támogatást nyújtani az Adatkezelő szervezeti egység részére az incidenssel érintettek tájékoztatásában.

A biztonsági vezetőnek kapcsolattartóként kell szolgálnia a Hatóság felé:

- szakmai kérdésekben konzultációt kell folytatnia a Hatósággal, különös tekintettel a hatásvizsgálatra,
- a Hatóság által indított vizsgálatokban, eljárásokban közre kell működnie,
- A biztonsági vezetőnek a Társaság adatkezeléseinek valamennyi érintettje számára elérhetőnek kell lennie a Társaság honlapján-, illetve az adatkezelési tájékoztatókban feltüntetett elérhetőségein keresztül.

Amennyiben az érintettektől érkező megkeresések kezelése érdekében az Adatkezelő szervezeti egység a biztonsági vezető szakmai segítségét kéri, úgy a biztonsági vezető köteles a szakmai segítséget megadni.

Ha az érintett vitatta az Adatkezelő szervezeti egység eljárásának jogszerűségét, úgy a biztonsági vezetőnek vizsgálatot kell folytatnia. Amennyiben a biztonsági vezető vizsgálata eredményeként beigazolódik, hogy az adatkezelő nem megfelelően járt el, úgy fel kell, hogy szólítsa az Adatkezelő szervezeti egységet a jogszerű állapot visszaállítására.

4.4.3 A Biztonsági szervezet információbiztonsági szakértőjének feladata

Az Adatkezelő szervezeti egység kérésére, adatbiztonsági kérdésekben szakmai támogatást kell nyújtania az adatkezeléssel járó szakmai folyamatok-, és az adatvédelmi hatásvizsgálat felülvizsgálatához, valamint az incidenskezeléshez.

A Biztonsági szervezet Információbiztonsági szakterülete, feladatkörében,

- éves tervben meghatározott, vagy
- biztonsági eseményre reagálva, vagy
- a technológia fejlődéséből adódóan ismerté vált sérülékenységekre reagálva, ellenőrzéseket végez.

Amennyiben adatbiztonsági szempontból hiányosságokat állapít meg, felhívja az Adatkezelő figyelmét a szabálytalanságok megszüntetésére, amelynek megvalósulásához szakmai segítséget nyújt.

A biztonsági vezető vagy az Adatkezelő szervezeti egység kérésére az adatvédelmi incidens kivizsgálásában és mérlegelésében - amennyiben az adatbiztonsági szakmai kérdést érint - a Biztonsági szervezet információbiztonsági szakértője szakmai segítséget kell, hogy nyújtson.

4.4.4 Informatika szervezet

A biztonsági vezető vagy az Adatkezelő szervezeti egység kérésére az adatvédelmi incidens kivizsgálásában és mérlegelésében - amennyiben az informatikai szakmai kérdést érint – az Informatika szervezet szakmai segítséget kell, hogy nyújtson.

4.5 Az adatkezelés lezárása

4.5.1 Az Adatkezelő szervezeti egység feladata

Amennyiben az Adatkezelő szervezeti egység az adatkezeléssel járó tevékenységét megszünteti, döntenie-, és gondoskodnia kell arról, hogy az adatok végleges törlésre és/vagy archiválásra és/vagy anonimizálásra kerüljenek.

Az Adatkezelő szervezeti egységnek dokumentálnia (3. sz. melléklet) kell az adott adatkezelés lezárásának tényét, és ezt meg kell küldenie a biztonsági vezető részére is.

4.5.2 A biztonsági vezető feladata

Az Adatkezelő szervezeti egység által megküldött (3. sz. melléklet) „Adatlap adatkezelési tevékenységek nyilvántartásához” adatlap adatait át kell, hogy vezesse a Belső adatvédelmi nyilvántartásba.

5.0 HIVATKOZÁSOK, MÓDOSÍTÁSOK HATÁLYON KÍVÜL HELYEZÉSEK

5.1 Hivatkozások

A szabályozás az alábbi jogszabályokra, ajánlásokra és irányelvekre, belső szabályozásokra alapozva, azokkal teljes összhangban, azoknak megfelelően és az azokban foglalt célok betartása érdekében került kialakításra:

- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (GDPR),
- Magyarország Alaptörvénye,
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.),
- Az Európai Adatvédelmi Biztos (EDPS - European Data Protection Supervisor), Európai Adatvédelmi Testület (korábban: WP29-es munkacsoport, EDPB - European Data Protection Board), és a Nemzeti Adatvédelmi és Információszabadság Hatóság által meghozott határozatok, kiadott iránymutatások, ajánlások, tájékoztatók és közlemények,
- A munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.)
- A polgári törvénykönyvről szóló 2013. évi V. törvény (Ptk.)
- A Társaságok mindenkor hatályos Szervezeti és Működési Szabályzata (SZMSZ)
- A Társaságok mindenkor hatályos Informatikai Biztonsági Szabályzata (IBSZ)
- A Társaságok mindenkor hatályos Védendő információinak kezeléséről szóló szabályzata

5.2 Módosítások

Jelen utasításhoz nincsenek.

5.3 Hatályon kívül helyezések

Jelen utasításhoz nincsenek.

5.4 Magyar Vagon Business Solutions Kft. tájékoztatása

Az utasítást a Magyar Vagon Business Solutions Kft. részére **meg kell küldeni**/nem kell megküldeni.

5.5 Rendelkezések

Jelen utasításhoz nincsenek.

6.0 HATÁLYBA LÉPTETÉS

Az utasítás a közzétételt követő napon lép hatályba.

7.0 MELLÉKLETEK, BIZONYLATOK

7.1 Mellékletek

1. számú melléklet: „Adatvédelmi hatásvizsgálat” mintája

2. számú melléklet: „Érdelmérlegelési teszt” mintája
3. számú melléklet: „Adatlap adatkezelési tevékenységek nyilvántartásához” mintája
4. számú melléklet: „Adatkezelési tájékoztató” mintája
5. számú melléklet: „Adatvédelmi Incidens nyilvántartás” mintája

7.2 Bizonylatok

Jelen utasításhoz nem tartoznak bizonylatok.

Adatvédelmi hatásvizsgálat

1. Projektnév, szerepkörök:

Projektnév, és szerepkörök meghatározása a hatásvizsgálatban (készítő, felülvizsgáló, jóváhagyó)

2. Adatkezelés leírása:

Az adatkezelés rövid bemutatása, különösen az adatkezelés célja, jogalapja, kezelt adatok köre és egyéb lényeges körülmények.

Az adatkezeléshez kapcsolódó felelősségi viszonyok bemutatása. Az adatkezelésben közreműködő felek, adatkezelő, adatfeldolgozó közös adatkezelő, ezek egymáshoz való viszonya, és felelősségi körök megoszlása.

Rendelkezik-e az adatkezelésre alkalmazandó valamilyen szabvánnyal? Szabványok, magatartási kódexek, tanúsítványok felsorolása, amennyiben vannak ilyenek.

3. Adatok, adatkezelés folyamata:

A kezelt személyes adatok köre. Sorolja fel a gyűjtött és kezelt adatokat. Egyenként határozza meg a tárolás időtartamát, a címzetteket és azokat a személyeket, akik az adatokhoz hozzáférnek.

Az adatkezelési folyamatok bemutatása. Mutassa be az adatkezelés folyamatát (az adatgyűjtéstől az adatok megsemmisítéséig, az adatkezelés különböző szakaszait, a tárolást stb.), használjon például a személyes adatok útját - adatfolyamot - bemutató ábrát (melyet mellékletként feltölthet).

Melyek a személyes adatok kezelésére szolgáló eszközök? Sorolja fel a személyes adatok kezelésére szolgáló eszközöket (operációs rendszerek, alkalmazások, adatbázis-kezelő rendszerek, helyiségek, egyéb eszközök stb.)

4. Adatkezelés célja, jogalapja, tárolás időtartama:

Az adatkezelés céljai meghatározottak-e, egyértelműek-e és jogszerűek-e? Fejtse ki, hogy mitől meghatározottak, egyértelműek és jogszerűek az adatkezelés céljai.

Mi az adatkezelés jogalapja? Ismertesse az adatkezelés jogalapját (hozzájárulás, szerződés teljesítése, jogi kötelezettség teljesítése, létfontosságú érdekek védelme stb.)

A gyűjtött adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak-e, valamint a szükségesre korlátozódnak-e (adattakarékosság)? Mutassa be, hogy az egyes gyűjtött adatok miért szükségesek az adatkezelés céljára.

Pontosak-e az adatok, naprakész állapotban tartják-e azokat? Ismertesse az adatminőséget biztosító intézkedéseket.

Mi az adatmegőrzés időtartama? Mutassa be, hogy milyen jogi követelmények és/vagy adatkezelési szükségletek indokolják a tárolás időtartamát.

5. Az érintettek jogainak biztosítása:

Milyen módon tájékoztatják az érintetteket az adatkezelésről? Ismertesse az érintetteknek adott tájékoztatást és annak módját.

Amennyiben az adatkezelés hozzájáruláson alapul, milyen módon szerzik be az érintettek hozzájárulását? Mutassa be az annak biztosítására szolgáló eljárásokat, hogy az érintettek hozzájárulásának beszerzése megtörténik.

Milyen módon érvényesíthetik az érintettek a hozzáférési, illetve az adathordozhatósághoz való jogukat? Ismertesse azokat az intézkedéseket, amelyek biztosítják, hogy az érintettek hozzáférhessenek az adataikhoz, megkapják és továbbíthassák azokat.

Hogyan gyakorolhatják az érintettek a helyesbítéshez és törléshez való jogukat? Ismertesse azokat az intézkedéseket, amelyek biztosítják, hogy az érintettek helyesbíttethessék és töröltethessék adataikat.

Hogyan gyakorolhatják az érintettek az adatkezelés korlátozásához, valamint tiltakozáshoz való jogukat? Ismertesse azokat az intézkedéseket, amelyek biztosítják, hogy az érintettek kérhessék az adatkezelés korlátozását, illetve tiltakozhassanak személyes adataik kezelése ellen.

Az adatfeldolgozók kötelezettségeit egyértelműen rögzíti-e az adatfeldolgozási szerződés? Ismertesse az egyes adatfeldolgozók kötelezettségeit (időtartam, hatás, célok, utasítások a feldolgozóknak, stb.) illetve jelölje meg azok feladatait és kötelezettségeit meghatározó szerződéseket, magatartási kódexeket, és tanúsítványokat.

Az Európai Unión kívülre történő adattovábbítás esetén megfelelő védelemben részesülnek-e a személyes adatok? Nevezze meg mindazokat az EU-n kívüli országokat, amelyekben adatkezelés és adattárolás történik, továbbá jelölje meg, hogy azok megfelelő védelmi szintet biztosítanak-e (más esetben is írja le az adattovábbításra vonatkozó rendelkezéseket.)

6. Kockázatok, tervezett vagy meglévő intézkedések:

Tervezett vagy meglévő intézkedések az adatkezelésből adódó kockázatok mérséklése érdekében.

Logikai biztonságvédelem

Titkosítás

Anonimizálás

Az adatok különválasztása

Logikai hozzáférés szabályozás

Nyomon követhetőség (naplózás)

Archiválás

Papír alapú dokumentumok biztonsága

Adatminimalizálás

Fizikai biztonságvédelem

Üzembiztonság

Rosszindulatú szoftverek kiszűrése

A munkaállomások kezelése

Webhelybiztonság

Biztonsági mentés

Karbantartás

Adatfeldolgozók igénybevétele során alkalmazandó követelmények

Hálózatbiztonság

Fizikai hozzáférésvédelem

Hálózati tevékenységek megfigyelése

Hardverbiztonság

A kockázatforrások elkerülése

A nem emberi eredetű kockázatokkal szembeni védelem

Szervezeti védelmi intézkedések

Szervezet

Szabályzatok

Adatvédelmi kockázatok kezelése

Az adatvédelem beépítése a projektekbe

A személyes adatokkal kapcsolatos jogsértések kezelése

Humánerőforrás-menedzsment

Kapcsolat harmadik felekkel

Felügyelet

7. Kockázatok, jogosulatlan hozzáférés, megváltoztatás, adatvesztés:

Az adatokhoz való jogosulatlan hozzáférés

Milyen főbb következményekkel járna az érintetteknek, ha a kockázat bekövetkezne?

Mely fő fenyegető veszélyek idézhetik elő a kockázatot?

Melyek a kockázat forrásai?

A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?

Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

Az adatok véletlen vagy jogellenes megváltoztatása

Milyen főbb következményekkel járna az érintetteknek, ha a kockázat bekövetkezne?

Mely fő fenyegető veszélyek idézhetik elő a kockázatot?

Melyek a kockázat forrásai?

A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?

Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

Adatvesztés

Milyen főbb következményekkel járna az érintettek, ha a kockázat bekövetkezne?

Mely fő fenyegető veszélyek idézhetik elő a kockázatot?

Melyek a kockázat forrásai?

A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?

Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

8. Biztonsági vezető véleménye:

Biztonsági vezető véleménye, esetleges korrekciós javaslatok.

9. Az érintettek véleménye:

Az érintettek véleményének kikérése megtörtént-e, és ha nem, akkor miért nem?

Az érintettek véleménye? Vélemények összegyűjtésének és elemzésének módja.

10. Az Adatkezelő szervezeti egység:

Biztonsági vezető jóváhagyása, esetleges korrekciós javaslatok.

Az Adatkezelő szervezeti egység vezetője igazolja, hogy

- az adatkezelés körülményeinek a leírása megfelel a valóságnak.
- a kockázatokat a tervezett és meglévő intézkedések szerint vette tekintetbe.

Jóváhagyja a jelzett korrekciós intézkedéseket.

Vállalja a jelzett korrekciós intézkedések mihamarabbi megvalósítását.

Érdedmérlegelési teszt

1. Az érdedmérlegelési teszt elvégzésének oka:

Annak bemutatása, hogy a személyes adatok kezelése elengedhetetlen a cél elérése érdekében:

- igazolni és dokumentálni szükséges, hogy nincs olyan alternatív megoldás, amely személyes adatok kezelése nélkül alkalmas lenne a cél elérésére

Annak bemutatása, hogy a GDPR 6. cikk (1) bekezdése a)- f) pontjai közül kizárólag az f) pont, azaz a jogos érdek képezi az adatkezelés alapját:

- igazolni és dokumentálni szükséges, hogy a jogalapok közül, kizárólag a jogos érdek alkalmazható

2. A Társaság, mint adatkezelő jogos érdeke:

A kellően konkrét jogos érdek bemutatása:

- azon jogszabályhelyek felsorolása, amelyek lehetővé és nem kötelezővé teszik az adatkezelést
- társadalmi-, üzleti-, gazdasági érdekek kifejtése.

3. Az adatkezelés célja, milyen személyes adatok, mennyi ideig tartó adatkezelését igényli a jogos érdek:

Az adatkezelés célja:

A kezelt személyes adatok köre:

Adatkezelés időtartama:

4. Az Érintett érdekei, alapjogok:

Az Érintettek, mint természetes személynek jogszabályokon (GDPR, Alaptörvény, Infotv, Ptk., stb.) alapuló, az adatkezeléssel érintett, védelmet élvező érdekének, jogosultságainak meghatározása.

Az Érintettnek, mint természetes személynek az előbbieket szerinti védelmet élvező érdeke fűződik ahhoz, hogy:

- információs önrendelkezési jogát gyakorolhassa,
- saját személyes adatainak mások általi kezeléséről maga rendelkezessen,
- magánszféráját az adatkezelők tiszteletben tartsák,
- az információs önrendelkezési jog érvényesítését elősegítő, illetve a személyes adatok és ezen keresztül a magánszféra védelmét biztosító jogszabályi rendelkezések érvényesüljenek.

Az adatkezelésből eredő, Érintettre kiható azon következmények összegyűjtése, amelyek az Érintett érdekeit szolgálják, rá nézve pozitív hatásként jelentkeznek.

5. A Társaság jogos érdekeinek és az Érintettek érdekeinek, alapjogainak súlyozása:

Súlyozás a 2-es és 4-es pont összevetésével.

6. A biztosítékok, garanciák:

Mindazoknak a biztosítékoknak és garanciáknak a felsorolása, melyek az adatkezelés alapelveinek érvényesülését elősegítik, továbbá annak alátámasztása, hogy az érintett adatkezeléssel kapcsolatban felmerült érdekeinek, jogainak korlátozása a szükségesség, arányosság elvének érvényesülése mellett történt.

Érintetti jogok biztosítására hozott intézkedések:

Az érintetti jogok (pl.: előzetes tájékoztatás, hozzáférési jog, tiltakozás, helyesbítés) biztosítására hozott intézkedések kifejtése, az átláthatóság elvének érvényesülése érdekében.

Biztonsági intézkedések:

Azoknak a technikai és szervezési intézkedéseknek a kifejtése, amelyek az adatok biztonságos kezelését garantálják.

Jogorvoslati lehetőségek feltüntetése:

Belső- és külső csatornák feltüntetése. (biztonsági vezető, bíróság, hatóság)

7. Az érdekmérlegelési teszt eredménye:

A fent kifejtettek összefoglalása, az érdekmérlegelési teszt végeredményeképpen az adatkezelő jogos érdeke vagy az érintett jogos érdeke elsőbbségének meghatározása, az eredmény dokumentálása.

Adatlap
adatkezelési tevékenységek nyilvántartásához

.....
(adatkezelési tevékenység megnevezése)

A következő adatokat az adatkezelési tevékenységet végző szervezeti egység tölti ki:

1. Adatkezelési tevékenységet végző szervezeti egység*:

(*Amennyiben az adatkezelési tevékenységet több szervezeti egység együtt végzi, akkor az összes szervezeti egység feltüntetésére van szükség.)

szervezeti egység neve	
címe	
telefonszáma	
e-mail címe	
kapcsolattartó neve	
kapcsolattartó telefonszáma	
kapcsolattartó e-mail címe	

2. Adatkezelés megkezdésének tervezett időpontja:

dátum	
-------	--

3. Adatkezelés célja*:

(*Az adatok felhasználásának tényleges indokát kell megjelölni, túl általános adatkezelési cél meghatározása pl. munkahelyi ellenőrzés, IT biztonság, közérdekű feladat végrehajtása; nem megfelelő)

adatkezelés célja	
-------------------	--

3.1. Az adatkezelés kapcsolódik -e más, már folyamatban lévő adatkezeléshez?

Igen	Nem
------	-----

Ha igen, adja meg a kapcsolódó adatkezelés megnevezését!

megnevezés	
------------	--

4. Adatkezeléssel érintett személyes adatok*:

(*pl. név, lakcím, anyja neve, születési helye- és ideje, törzsszáma, telefonszáma, e-mail címe)

kezelt személyes adatok megnevezése	
-------------------------------------	--

5. Az adatkezeléssel érintettek köre, száma:

adatkezeléssel érintettek köre	
adatkezeléssel érintettek (hozzávetőleges) száma	- 1 1 - 50 50 - 100

	100 - 500
	500 - 1000
	1000 -

5.1. Az adatkezelésben érintett-e?

adatkezelő munkavállalója	Igen	Nem
adatkezelő munkavállalójának családtagja	Igen	Nem
gyermek	Igen	Nem

6. Az adatok forrása:

érintettől felvett	
nem az érintettől felvett	

6.1. Amennyiben a személyes adatokat nem az érintettől gyűjtik, akkor kérem, hogy adja meg az adatok forrását!

adatok forrása	
----------------	--

6.2. Hogyan kerül a kezelésünkbe a személyes adat?

adatgyűjtés módja	
-------------------	--

7. Címzett*:

(*A személyes adatok továbbítása, vagy az azokhoz történő hozzáférés biztosítása.)

továbbított személyes adatok fajtája	
címzett megnevezése	
címe	
telefonszáma	
e-mail címe	
címzett adatkezelői minősége* (*címzett lehet önálló adatkezelő, közös adatkezelő, adatfeldolgozó)	
adattovábbítás módja	papír alapú elektronikus hozzáférés biztosítás
adattovábbítás gyakorisága	eseti rendszeres

7.1. Megvalósul-e harmadik országba/nemzetközi szervezet részére történő továbbítás?

harmadik országba történő adattovábbítás	Igen	Nem
nemzetközi szervezet részére történő adattovábbítás	Igen	Nem
amennyiben igen, akkor milyen garancia alapján		

8. Adatkezelés időtartama*:

(*Mennyi ideig kezeljük az adatot? Mikor kerül törlésre? A kezelésre, törlésre vonatkozóan van-e jogszabályi előírás? Ha van annak megjelölése szükséges.)

adatkezelés időtartama, vagy az időtartam meghatározásának szempontjai	
kezelésre, törlésre vonatkozó jogszabályi előírás megjelölése	

9. Kezeln kívánt adatok tárolási helye?

elektronikus rendszerben	
manuális tárolás	

9.1. Ha elektronikus, mely rendszer(ek)ben kezelik a személyes adatokat?

elektronikus rendszer neve	
----------------------------	--

9.2. Manuális tárolás esetén, hol található a személyes adat?

iroda/szoba/írártár/egyéb	
---------------------------	--

10. Az adatkezelésre vonatkozóan készült- e adatkezelési tájékoztató?

Igen	Nem
------	-----

11. Adatkezelői minőség:

önálló adatkezelő (adatkezelő az adatkezelést önállóan végzi)	
közös adatkezelés (adatkezelő az adatkezelést más adatkezelővel együtt végzi)	
adatfeldolgozó (adatkezelő adatfeldolgozói feladatot lát el, más adatkezelő megbízásából)	

11.1. Közös adatkezelés esetén:

közös adatkezelő szervezet megnevezése	
címe	
telefonszáma	
e-mail címe	
kapcsolattartó neve	
kapcsolattartó telefonszáma	
kapcsolattartó e-mail címe	
adatvédeleми tisztviselő neve	
adatvédeleми tisztviselő címe	
adatvédeleми tisztviselő e-mail címe	
közös adatkezelésre irányuló szerződés (tervezet) készült	Igen Nem

11.2. Adatfeldolgozó igénybevétele esetén:

adatfeldolgozó megnevezése	
címe	
telefonszáma	
e-mail címe	
kapcsolattartó neve	
kapcsolattartó telefonszáma	
kapcsolattartó e-mail címe	
adattvédeleml tiszttviselő neve	
adattvédeleml tiszttviselő címe	
adattvédeleml tiszttviselő e-mail címe	
adatfeldolgozó milyen tevékenységet végez	
adatfeldolgozás helye	
adatfeldolgozás technológiája	
adatfeldolgozóll tevékenység végzésének időtartama	
adatfeldolgozóll szerződés (tervezet) készült	Igen Nem

12. Adatkezeléssel érintett személyes adatok:**12.1. Az adatkezelési tevékenység során megvalósul-e a személyes adatok különleges kategóriáinak kezelése?**

Igen	Nem
------	-----

12.2. Ha igen, melyekre?

faji vagy etnikai származásra vonatkozó adat	
politikai véleményre vonatkozó adat	
vallási vagy világnézeti meggyőződésre utaló adat	
szakszervezeti tagságra utaló adat	
genetikai adat	
biometrikus adat	
egészségügyi adat	
szexuális életre/szexuális irányultságra vonatkozó adat	

12.3. Az adatkezelés céljának eléréséhez mindenképpen szükségesek-e a kezelni kívánt személyes adatok?

Igen	Nem
------	-----

13. Adatkezelés jogalapja:

a)	Rendelet 6. cikk (1) a) – az érintett hozzájárulása	
b)	Rendelet 6. cikk (1) b) – szerződés megkötéséhez, teljesítéséhez szükséges* (*a szerződésben az érintett az egyik fél)	
c)	Rendelet 6. cikk (1) c) - jogi kötelezettség teljesítése	
d)	Rendelet 6. cikk (1) d) – az érintett vagy más természetes személy létfontosságú érdekének védelme	
e)	Rendelet 6. cikk (1) e) – közérdekű feladat ellátása, közhatalmi jogosítvány gyakorlása	
f)	Rendelet 6. cikk (1) f) – jogos érdek	

13.1. Amennyiben az adatkezelés jogalapja 6. cikk (1) a) pont, a hozzájárulás megadása megfelel-e a Rendeletben meghatározott feltételeknek, azaz önkéntes, konkrét, egyértelmű kinyilvánítás, amely megfelelő tájékoztatáson alapul?

Igen	Nem
------	-----

13.1.1. Érintetti hozzájárulás megadásának módja?

érintett nyilatkozata	
megerősítést félreérthetetlenül kifejező cselekedet	

13.1.2. Az érintetti hozzájárulás visszavonásának lehetősége hogyan biztosítható?

--

13.2. Amennyiben az adatkezelés jogalapja 6. cikk (1) c) vagy e) pont az adatkezelésre vonatkozó jogszabály címe és a pontos jogszabály hely megnevezése:

jogszabály címe, pontos jogszabályhely	
--	--

13.3. Személyes adatok különleges kategóriáinak kezelése esetén mely feltételek érvényesülnek az alábbiak közül?

(*különleges személyes adatok kezelése esetén a 6. cikk (1) a)-f) pontok valamelyikének fennállása mellett, az alábbi feltételek valamelyikének teljesülése is szükséges a jogszerű adatkezeléshez)

érintett kifejezett hozzájárulása	
foglalkoztatást, szociális biztonságot szabályozó jogi előírásokból fakadó kötelezettség teljesítése	
érintett létfontosságú érdeke	
egyesület vagy nonprofit szervezet tevékenysége	
különleges adatok érintett általi kifejezett nyilvánosságra hozatala	
jogi igények előterjesztése, érvényesítése, védelme, illetve igazságszolgáltatási tevékenység	
jelentős közérdek	
egészségügyi ellátás, munkahelyi alkalmasság	
népegészségügy területét érintő közérdek	
közérdekű archiválás, történelmi kutatás, statisztikai cél	

13.4. Gyermek adatainak kezelése esetén készült-e szülői hozzájáruló nyilatkozat?

Igen	Nem
------	-----

14. Adattovábbítás jogalapja*

(*A személyes adatok továbbítása, vagy az azokhoz történő hozzáférés biztosítása.)

adattovábbítás jogalapja	
--------------------------	--

14.1. Harmadik országba/nemzetközi szervezet részére történő adattovábbítás jogalapja:

adattovábbítás jogalapja	
--------------------------	--

15. Adatok törlésére vonatkozó információk

az adatkezelés megszűnését követően milyen módon kerülnek törlésre a személyes adatok?	
hogyan történik az adattörlés dokumentálása?	

16. Az adatkezeléssel kapcsolatban felmerülhet-e kockázat?

Igen	Nem
------	-----

16.1. Ha igen, milyen kockázatok merülhetnek fel? *

(*Több lehetséges válasz esetén azok mind megjelölendők.)

- hátrányos megkülönböztetés

- személyazonosság-lopás
- személyazonossággal való visszaélés
- pénzügyi veszteség
- jó hírnév sérelme
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése
- álnevesítés engedély nélkül történő feloldása
- egyéb jelentős gazdasági vagy szociális hátrány
- az érintettek nem gyakorolhatják jogaikat és szabadságaikat
- az érintettek nem rendelkezhetnek saját személyes adataik felett

- olyan adatok kezelése történik, amelyek faji vagy etnikai származásra;
- politikai véleményre;
- vallási és világnézeti meggyőződésre;
- szakszervezeti tagságra utalnak;
- a kezelt adatok genetikai adatok,
- egészségügyi adatok,
- szexuális életre;

- büntetőjogi felelősség megállapítására;
- bűncselekményre;
- fentiekhez kapcsolódó biztonsági intézkedésekre vonatkoznak,

- személyes jellemzők értékelésére
- így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők,
- gazdasági helyzet,
- egészségi állapot,
- személyes preferenciák vagy érdeklődési körök,
- megbízhatóság vagy viselkedés,
- tartózkodási hely vagy mozgás elemzésére, vagy előrejelzésére kerül sor személyes profil létrehozása avagy felhasználása céljából,

- kiszolgáltatott személy személyes adatai,
- gyermekek személyes adatai
- az adatkezelés nagy mennyiségű személyes adat alapján zajlik
- nagyszámú érintettre terjed ki.

16.1.1. A felmerülő kockázat(ok) milyen károkat okozhat?

fizikai kár	
vagyoni kár	
nem vagyoni kár	

17. Milyen intézkedések megtételével csökkenthetők a felmerülő/azonosított kockázatok?

intézkedés megnevezése	
------------------------	--

18. Milyen intézkedések szükségesek az adatok biztonságának megőrzése érdekében?

intézkedés megnevezése	
------------------------	--

19. Amennyiben az adatkezelés jogalapja 6. cikk (1) f) – jogos érdek, akkor elkészült-e az érdekmérlegelési teszt?

Igen	Nem
------	-----

20. Az adatkezelés megkezdését megelőzően szükséges-e adatvédelmi hatásvizsgálat lefolytatása?*

(*Rendelet 35. cikk szerinti feltételek fennállása esetén + NAIH lista.)

Igen	Nem
indoklás	

21. Ki, milyen módon adja meg az érintettek részére a tájékoztatást?*

(*pl. honlapon közzétett, papír alapon átadott, hírlevélben, szabályzatban, utasításban kiadott)

tájékoztatás megadásának módja	
--------------------------------	--

A következő adatokat a biztonsági vezető tölti ki:

Belső adatvédelmi nyilvántartásba vétel*

(* a biztonsági vezető által vezetett Belső adatvédelmi nyilvántartásba vétel adatai)

Sorszám:	
Belső adatvédelmi nyilvántartásba vétel dátuma:	

Fogalom jegyzék

1. Rendelet: AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet);

2. 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;

3. érintett: bármely olyan meghatározott természetes személy, aki személyes adata alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható;

4. 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;

5. 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;

6. közös adatkezelők: ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg, azok közös adatkezelőknek minősülnek. A közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban határozzák meg a Rendelet szerinti kötelezettségek teljesítéséért fennálló, különösen az érintett jogainak gyakorlásával és a 13. és a 14. cikkben említett információk rendelkezésre bocsátásával kapcsolatos feladataikkal összefüggő felelősségük megoszlását, kivéve azt az esetet és annyiban, ha és amennyiben az adatkezelőkre vonatkozó felelősség megoszlását a rájuk alkalmazandó uniós vagy tagállami jog határozza meg. A megállapodásban az érintettek számára kapcsolattartót lehet kijelölni;

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

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

9. 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;

10. különleges adat: a személyes adatok különleges kategóriába 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;

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

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

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

14. adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

15. 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;

16. 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;

17. harmadik ország: minden olyan állam, amely nem EGT-állam;

18. nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre;

19. adattörlés: az adat felismerhetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

20. adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

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

22. adatvédelmi hatásvizsgálat: az adatkezelés előzetes kontrollja, a személyes adatok kezeléséből eredő, a természetes személyek jogait és szabadságait érintő kockázatok feltárása és az azonosított kockázatok mérséklésére teendő intézkedés értékelése.

**Adatkezelési tájékoztató a ... (érintett Társaság neve) által
a ...[Ide kell beírni az adatkezelést, amire a tájékoztató vonatkozik] összefüggésben végzett
adatkezelésről**

1. Az adatkezelő megnevezése

Név:

Székhely:

Cégjegyzékszám:

Adószám:

E-mail: ...[Az adatkezelő szervezeti egység által az adatkezeléssel kapcsolatban használt e-mail cím, vagy a szervezeti egység e-mail címe.]

a továbbiakban: **Adatkezelő**

Adatkezelő adatvédelmi kérdésekben az alábbi elérhetőségeken kereshető:

E-mail: adatvedelem@mavag.hu

Postai cím: 1139 Budapest, Lomb utca 37-39.

2. Adatfeldolgozó megnevezése

[Amennyiben az adatkezelés során az adatok feldolgozására, tárolására harmadik személy kerül bevonásra, akkor ebben a pontban kell azt szerepeltetni.

Egyéb esetben a ponthoz javasolt a következő szövegezés alkalmazása.

„Adatkezelő ezen adatkezelés során külső adatfeldolgozó tevékenységét nem veszi igénybe.”]

Név:

Székhely:

Cégjegyzékszám:

Adószám:

E-mail:

a továbbiakban: **Adatfeldolgozó**

Adatvédelmi tisztviselő elérhetősége:

E-mail:

Az Adatkezelő és az Adatfeldolgozó között létrejött szolgáltatási szerződés alapján az Adatfeldolgozó teljes körű informatikai szolgáltatást nyújt az Adatkezelő részére, amely magába foglalja az elektronikus úton végzett adatkezelés során kezelt személyes adatok tárolásához szükséges tárhelyszolgáltatást és az egyes az adatok tárolására szolgáló szoftverek üzemeltetését.

[A példaként leírt szövegrész csak az elektronikusan végzett adatkezelésekre vonatkozik, de ha olyan adatkezelésről van szó, amelynél a papír alapú dokumentumokat is kezeli az Adatfeldolgozó, akkor ezt is javasolt megfogalmazni a teljes körű és átlátható tájékoztatás érdekében.

Amennyiben az Adatfeldolgozó az adott adatkezelés során az Adatkezelő részére egyéb szolgáltatást is nyújt, akkor azokat is fel kell sorolni a teljes körű és átlátható tájékoztatás érdekében.

Például: Humánerőforrás menedzsment, pénzügyi, számviteli szolgáltatás.]

3. Az érintett személye:

Valamennyi természetes személy, aki ... [Az érintettek kategóriáit itt kell definiálni. Az érintett az adott adatkezeléssel érintett személy és az adatkezelést végző munkatársaink is ide tartoznak.]

4. Az adatkezelésre vonatkozó információk

[Amennyiben egy adatkezelési folyamatban egymástól elkülöníthető célokból is történik az adatkezelés, úgy a 4. pontot szét kell bontani célonként alpontokra (4.1., 4.2., stb.) és mindegyik cél esetén meg kell jeleníteni az itt felsorolt információkat.]

Az adatkezelés célja: ... [A cél pontos, konkrét megjelölése. Nem megfelelő a cél megjelölése, ha az túl általános. Az adatkezelés célját az adatkezelés jogalapjára hivatkozással kell meghatározni.]

Az adatkezelés jogalapja: ... [Az adatkezelés jogszerűségének alátámasztása.

A GDPR 6. cikk (1) bekezdésének felsorolása alapján kell meghatározni, illetve, amennyiben különleges adat adatkezelését is végzik, akkor a 9. cikk (2) bekezdés alapján fennálló többletfeltétel megjelölése is szükséges.

Egy adatkezeléshez minden esetben csak egy jogalapot lehet meghatározni. Amennyiben több jogalap is felmerül, akkor fel kell mérni, hogy melyik fedi le teljes mértékben az adatkezelést.

+ A GDPR 6. cikk (1) bekezdés a) alpontja, az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez jogalap munkavállalók adatainak munkáltatással kapcsolatos kezelése esetén nem alkalmazható.

A hozzájárulás jogalap akkor alkalmazható munkavállaló esetében, amikor nem munkáltatásról van szó.

Pl.: valamilyen rendezvényen történő részvételhez, amikor a munkavállaló saját döntése szerint jelentkezik, vagy sportrendezvényen részt vételhez ajándék póló, egyen mez, megkapásához a munkavállaló megadja a méretét.

Ezeknek az adatkezeléseknek a felismeréséhez a kulcs az, hogy a munkavállaló a saját, önálló, független döntése szerint adja meg az adatait.

+ ha az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés c) vagy e) pontja, akkor javasolt megjelölni azt a jogszabályi rendelkezést, amely az adatkezelést kötelezővé teszi.

+ Amennyiben az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés f) pont szerinti jogos érdek, úgy röviden (2-3 mondatban) ismertetni kell azt a jogos érdeket, amely megalapozza az adatkezelést.

+ Amennyiben egy jogszabály az adatkezelési kötelezettséget meghatározza, de nem írja elő pontosan az adatkezelésre vonatkozó szabályokat, illetve a kezelhető adatok körét, akkor az adatkezelésre vonatkozóan az Adatkezelő fogja ezeket meghatározni és az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés f) pont szerint az adatkezelés az adatkezelő jogos érdeke lesz.]

A kezelt adatok köre: ... [Az adatkezelés során kezelt személyes adatok pontos felsorolása szükséges.]

A személyes adatok forrása: ... [Azt szükséges feltüntetni, hogy az adatokat honnan vette fel az Adatkezelő. Pl.: az érintettől felvett]

Az adatkezelés időtartama: ... [Azt szükséges feltüntetni, hogy az adatokat Adatkezelő meddig kezeli. A pontos dátum, vagy időtartam, vagy egy adott eseménytől függően szövegesen is meghatározható.

Például:

- amennyiben hozzájárulás az adatkezelés jogalapja, akkor megfelelő időtartamként a „hozzájárulás visszavonásáig” meghatározás.
- ha szerződés teljesítéséhez szükséges a jogalap, akkor „a szerződés teljesítését követően a polgári jogi igény elévülési idejéhez igazodóan 5 évig.” meghatározás.
- munkaviszonyal kapcsolatos adatkezelés esetén „munkaviszony megszűnését követő 3 évig” (ez igazodik a munkajogi igény elévülési idejéhez), vagy „a nyugdíjkorhatár elérését követő 5 évig” (a Nyugdíjbizt. tv. alapján).

Ezek csak példák számtalan lehetőség lehet még az adatkezelés természetét figyelembe véve!]

Az adatkezelés módja: ... [Az adatkezelés történhet papír alapon, vagy elektronikusan.

Ha elektronikusan valamely rendszerben történik, akkor az informatikai rendszert kell megjelölni. Pl.: SAP IHIR]

Az adatok megismerésére jogosult személyek köre: ... [Annak meghatározása, hogy kik jogosultak az adatokat megismerni.]

Adattovábbítás: ... [Itt fel kell tüntetni azt, hogy az adatkezelés során kinek történik az adatok továbbítása, milyen célból és milyen jogalappal.

Minden a folyamatba beépített adattovábbítást fel kell tüntetni.

+ Nem számít adattovábbításnak dokumentumok előállításakor a számítógépen keletkezett állományok helyi, vagy központi szerver oldali tárolása.

+ Nem lehet előre felkészülni egyedi ismeretlen célú és időpontú hatósági ellenőrzésre, amely során a hatóság működésére vonatkozó jogszabályok alapján folytat ellenőrzés és kéri be az adatokat a hatóság.]

5. Adatbiztonsági intézkedésekről szóló tájékoztatás

- Adatkezelő az Adatfeldolgozó közreműködésével [Amennyiben nem történik elektronikus adatfeldolgozásra Adatfeldolgozó tevékenységének igénybe vétele, akkor „az Adatfeldolgozó közreműködésével” szövegrész törlendő] megteszi azokat a technikai és szervezési intézkedéseket:
 - a) amelyek ahhoz szükségesek, hogy az informatikai rendszerek az Informatikai biztonsági szabályzatban (IBSZ) foglaltaknak megfelelően működjenek;
 - b) amellyel biztosítja, hogy a jogosult felhasználók a jogosultsági szintjüknek megfelelően érhék el az informatikai rendszereket, azok funkcióit és az általuk kezelt adatokat;
 - c) amellyel gondoskodik az adatok mentéséről és archiválásról.
- Az Adatkezelő betartja azokat az eljárási szabályokat, amelyek az adatkezelésre vonatkozóan a 7. pontban meghatározott jogszabályokban foglalt előírások érvényre juttatásához szükségesek. Ezen jogszabályok betartását az Adatkezelő az Adatfeldolgozótól is elvárja a GDPR 28. cikk (3) bekezdés alapján kötött létrejött adatfeldolgozási szerződés alapján. [Amennyiben nem történik elektronikus adatfeldolgozásra Adatfeldolgozó tevékenységének igénybe vétele, akkor ez az utolsó mondat törlendő.]
- Az Adatkezelő az elektronikusan kezelt adatállományokat az Adatfeldolgozó útján [Amennyiben nem történik elektronikus adatfeldolgozásra Adatfeldolgozó tevékenységének igénybe vétele, akkor „az Adatfeldolgozó útján” szövegrész törlendő.] a vírusellenőrzésnek és egyéb biztonsági szűréseknek veti alá.
- Adatkezelő olyan műszaki, szervezési és szervezeti intézkedésekkel gondoskodik az adatkezelés biztonságának védelméről, amely az adatkezeléssel kapcsolatban a kockázatoknak megfelelő védelmi szintet nyújt, az alkalmazott informatikai eszközöket úgy választja meg és oly módon üzemelteti, hogy a kezelt adat:
 - a) az arra feljogosítottak számára hozzáférhető legyen (rendelkezésre állás);
 - b) hitelessége és hitelesítése biztosított legyen (adatkezelés hitelessége);
 - c) változatlanlansága igazolható legyen (adatintegritás);
 - d) csak az arra jogosult számára legyen hozzáférhető, a jogosulatlan hozzáférés ellen védett legyen (az adat bizalmassága).

6. Az érintettek jogai és jogérvényesítési lehetőségei

6.1. A tájékoztatás kéréséhez való jog

Az érintett tájékoztatást kérhet az Adatkezelőtől, kérheti személyes adatainak helyesbítését, valamint az adatkezelés korlátozását. Az érintett kérelmére az Adatkezelő tájékoztatást ad az általa kezelt adatokról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatkezelő nevééről, címéről (székhelyéről), az adatfeldolgozók nevééről, címéről (székhelyéről) és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi feladatok ellátásával megbízott munkavállaló elérhetőségéről, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az érintett személyes adatait, illetve az érintettet az adatkezeléssel összefüggő jogairól. Az Adatkezelő a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 1 hónapon belül írásban, közérthető formában adja meg a tájékoztatást. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. Amennyiben a

tájékoztatás kérése megalapozatlan vagy – különösen ismétlődő jellege miatt - túlzó, az Adatkezelő megtagadhatja a kérelem alapján történő intézkedést. Az Adatkezelő mindaddig megtagadhatja az érintetti jogainak gyakorlására irányuló kérelem teljesítését, ameddig az érintettet kétséget kizáróan nem tudja azonosítani.

6.2. Hozzáféréshez való jog

Az érintett jogosult arra, hogy az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e.

A hozzáférés joga alapján érintett jogosult arra, hogy a folyamatban lévő adatkezeléssel összefüggő személyes adatokhoz és az alábbi információkhoz hozzáférést kapjon:

- adatkezelés célja,
- az érintett személyes adatok kategóriái,
- az adatkezelés időtartama,
- arról, hogy kik és milyen célból kapják vagy kapták meg az érintett személyes adatait,
- az érintett adatkezeléssel összefüggő jogai,
- a felügyeleti hatósághoz címzett panasz benyújtásának joga.

Az érintett kérésére az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát – amennyiben az nem érinti hátrányosan mások jogait és szabadságait - rendelkezésére bocsátja. Az érintett által kért további másolatokért az Adatkezelő költségtérítést állapíthat meg.

6.3. Hozzájárulás visszavonásához való jog

[Ezt csak akkor kell szerepeltetni, ha az adatkezelés jogalapja az érintett hozzájárulása.]

Az érintett bármikor korlátozás nélkül visszavonhatja az adatkezeléshez adott hozzájárulását. Amennyiben az érintett visszavonja a hozzájárulást, úgy az adatkezelő a hozzájárulás alapján kezelt személyes adatokat törli. Tájékoztatjuk az érintettet, hogy a hozzájárulás visszavonása nem érinti a visszavonást megelőzően végzett adatkezelés jogszerűségét.

6.4. Az adatok módosításához, helyesbítéséhez és kiegészítéséhez való jog

[Mindig szerepeltetni kell!

De van olyan adatkezelés, amely esetében nem értelmezhető. Pl.: kép-, vagy hang-, valamint kép- és hangfelvétel esetén]

Az érintett az 1. pontban megadott elérhetőségen keresztül kérheti a rá vonatkozó pontatlan személyes adatainak módosítását (helyesbítését), illetve a hiányos személyes adatok kiegészítését. Adatkezelő a helyesbítésről értesíti az érintettet.

6.5. Az adatok törléséhez való jog („elfeledtetéshez való jog”)

[Mindig szerepeltetni kell!

Az adatok törléséhez való jog akkor is megilleti, ha a törlési kérelem a GDPR 17. cikk (3) bekezdésében foglalt valamely oknál fogva részben vagy egészben elutasításra kerül.

Ebben az esetben a törlés nem alkalmazandó, azonban a kérelmező érintettet tájékoztatni kell a törlés elutasításáról és annak indokairól.

A törlés akkor nem alkalmazandó amennyiben az adatkezelés szükséges:

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

Az érintett kérheti a személyes adatainak törlését, ha az adatkezelés célja megszűnt, ha az érintett visszavonja hozzájárulását ha azok adatok kezelése jogellenes, ha az adatok tárolásának meghatározott határideje lejárt, továbbá ha azt bíróság vagy hatóság elrendelte. Adatkezelő a személyes adatok törléséről értesíti az érintettet. Az Adatkezelő a személyes adatokat nem törli, ha azok az Adatkezelőre vonatkozó jogszabályi kötelezettség teljesítéséhez, továbbá jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükségesek.

6.6. Az adatok kezelésének korlátozásához való jog

Az Adatkezelő bármely elérhetőségén kérheti, hogy a személyes adatainak kezelését az Adatkezelő korlátozza amennyiben:

- az érintett vitatja a személyes adatok pontosságát (ez esetben a korlátozás arra az időtartamra vonatkozik, amíg az Adatkezelő ellenőrzi az adatok helyességét);
- az adatkezelés jogellenes, de az érintett ellenzi az adatok törlését és kéri azok felhasználásának korlátozását;
- az adatkezelés célja megszűnt, de az érintettnek szüksége van azokra jogi igények előterjesztéséhez, érvényesítéséhez, védelméhez.

A korlátozás addig tart, amíg azt az érintett által megjelölt indok szükségessé teszi. Ebben az esetben a személyes adatokat – a tárolás kivételével – csak az érintett hozzájárulásával; vagy jogi igények előterjesztéséhez, érvényesítéséhez, védelméhez; vagy más természetes vagy jogi személy jogainak védelme érdekében; vagy fontos közérdekből kezeljük. Az Adatkezelő az érintett kérésére történt korlátozás feloldásáról az érintettet előzetesen tájékoztatja.

6.7. Tiltakozáshoz való jog

[Akkor kell szerepeltetni, ha az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés e) vagy f) pontja.]

Amennyiben az Adatkezelő az adatkezelést a GDPR 6. cikk (1) bekezdés e) vagy f) pontja alapján végzi, úgy az érintett a megadott elérhetőségen keresztül tiltakozhat személyes adatainak kezelése ellen. Ez esetben az Adatkezelő a személyes adatait nem kezeli tovább, azokat törli. Az Adatkezelő az érintett személyes adatait a továbbiakban akkor kezelheti, ha az adatkezelést kényszerítő erejű jogos okok indokolják, továbbá ha azok jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükségesek.

6.8. Adathordozhatósághoz való jog

[Akkor kell szerepeltetni, amikor az adatkezelés a GDPR 6. cikk (1) bekezdés a) pontja vagy a 9. cikk (2) bekezdésének a) pontja szerinti hozzájáruláson, vagy a 6. cikk (1) bekezdésének b) pontja szerinti szerződésen alapul, valamint az Adatkezelő az adatkezelést automatizál módon végzi.]

Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, feltéve, hogy az adatkezelés a GDPR 6. cikk (1) bekezdés a) pontja vagy a 9. cikk (2) bekezdésének a) pontja szerinti hozzájáruláson, vagy a 6. cikk (1) bekezdésének b) pontja szerinti szerződésen alapul, valamint az Adatkezelő az adatkezelést automatizál módon végzi. Az érintett jogosult továbbá arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa. Az Adatkezelő kizárólag annak az adatkezelőnek továbbítja az érintett személyes adatait, amelyet azonosítható módon az érintett megjelöl. Az Adatkezelő az adattovábbítást követően a címzett adatkezelő által végzett adatkezelésért nem tartozik felelősséggel.

6.9. Jogorvoslathoz való jog

Jogainak megsértése esetén, vagy amennyiben az Adatkezelő döntésével nem ért egyet, panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál élhet:

Név: **Nemzeti Adatvédelmi és Információszabadság Hatóság**
Székhely: 1055 Budapest, Falk Miksa u. 9-11.
Postacím: 1363 Budapest, Pf. 9.
Telefon: +36 (1) 391-1400 / +36 (30) 683-5969 / +36 (30) 549-6838
Telefax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu

Jogainak megsértése esetén, vagy amennyiben az Adatkezelő döntésével nem ért egyet az Adatkezelővel szemben közvetlenül is fordulhat jogorvoslatért az Adatkezelő székhelye szerinti vagy a lakóhelye illetve tartózkodási helye szerinti bírósághoz. A bíróság az ügyben soron kívül jár el.

Amennyiben az adatkezeléssel kapcsolatban az Adatvédelmi tájékoztatóban foglaltakon kívül további információra van szüksége, akkor az Adatkezelő 1. pontban megadott elérhetőségén keresztül kérhet tájékoztatást.

Ha az érintettek a személyes adatai kezelésével kapcsolatban észrevétele, kifogása van, vagy az adatai kezeléséről tájékoztatást szeretne kérni, akkor azt az adatvédelmi feladatok ellátásával megbízott munkatársnál az adatvedelem@mavag.hu elérhetőségen teheti meg.

7. Releváns jogszabályok

[Meg kell jelölni minden az adatkezelés szempontjából releváns jogszabályt.]

- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet vagy GDPR),
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.),

Hatályos: 202 hónap napjától

(az adott Társaság nevének feltüntetésére)
Adatkezelő

Adatvédelmi Incidens nyilvántartás

sorszám	
incidens bejelentésének, feltárásának időpontja	
incidens bekövetkezésének vélelmezett időpontja	
érintett személyes adatok köre	
incidenssel érintettek köre	
incidenssel érintettek száma	
incidens jellege és körülményei	
incidens hatásai	
incidens elhárításra tett intézkedések	
incidens elhárításának időpontja	
az adatkezelést előíró jogszabályban meghatározott egyéb adatok	
érintett szervezeti egység	
ügyintéző/vizsgáló neve, elérhetősége	
kapcsolódó dokumentumok	
hatósági /fegyelmi eljárás, következmény, ennek adatai	
különleges adatot tartalmaz (I/N)	