34/2025. (IV.04. MÁV Ért. 6.) VIG sz. utasítás
a személyes adatok védelméről a MÁV-csoportban

MÓDOSÍTÁSOK JEGYZÉKE

Sorszám	Módosítások leírása	Módosítás dátuma	Módosította	Jóváhagyó

Készített: MÁV Zrt. Megfelelés támogatás

Jóváhagyó

Hegyi Zsolt
vezérigazgató

Tartalomjegyzék

1.0 AZ UTASÍTÁS CÉLJA 2

2.0 HATÁLY- ÉS FELELŐSSÉG MEGHATÁROZÁSA 3
2.1 Az utasítás személyi hatálya 3
2.2 Az utasítás tárgyi hatálya 3
2.3 Az utasítás kidolgozásáért és karbantartásáért felelős 3
3.0 FOGALMAK, RÖVIDÍTÉSEK ÉS TÁRGYSZAVAK 3
3.1 Fogalmak 3
3.2 Rövidítések 5
3.3 Tárgyszavak 5
4.0 AZ UTASÍTÁS LEÍRÁSA 5
4.1 A személyes adatok kezelésének általános szabályai 5
4.2 Az adatkezelésben közreműködők feladatai 6
4.3 A személyes adatok kezelésének kialakítása 9
4.4 Érintetti jogok gyakorlása 10
4.5 Az adattovábbítás szabályai 11
4.6 Adatfeldolgozás 11
4.7 Adatbiztonság 12
4.8 A személyes adatok törlése 15
4.9 Adatvédelmi incidens bekövetkezése esetén követendő eljárás 17
4.10 Nyilvántartások 20
4.11 Adatvédelmi hatásvizsgálat 21
5.0 HIVATKOZÁSOK, MÓDOSÍTÁSOK, HATÁLYON KÍVÜL HELYEZÉSEK 21
5.1 Hivatkozások 21
5.2 Hatályon kívül helyezések 22
6.0 HATÁLYBA LÉPTETŐ RENDELKEZÉS 22
7.0 MELLÉKLETEK, FÜGGELÉKEK JEGYZÉKE 22
7.1 Mellékletek 22
7.2. Függelékek 22

1.0 AZ UTASÍTÁS CÉLJA

Jelen utasítás célja, hogy meghatározza a MÁV-csoport által végzett adatkezelési tevékenységek rendjét, valamint biztosítsa az adatbiztonság követelményeinek érvényesülését.

2.0 HATÁLY- ÉS FELELŐSSÉG MEGHATÁROZÁSA

2.1 Az utasítás személyi hatálya

Az utasítás személyi hatálya kiterjed a MÁV-csoport valamennyi szervezeti egységére, munkavállalójára, továbbá a munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott személyekre, valamint a Társasággal szerződéses jogviszonyban álló természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre, a velük kötött szerződésekben rögzített mértékig.

2.2 Az utasítás tárgyi hatálya

Az utasítás tárgyi hatálya kiterjed a Társaság szervezeti egységeinél történő valamennyi személyes adat kezelésére.

2.3 Az utasítás kidolgozásáért és karbantartásáért felelős

Az utasítás kidolgozásáért és karbantartásáért a MÁV Zrt. Megfelelés támogatás szervezet vezetője felelős.

3.0 FOGALMAK, RÖVIDÍTÉSEK ÉS TÁRGYSZAVAK

3.1 Fogalmak

Adatbiztonság: az adatok jogosulatlan megismerése és kezelése (másolás, módosítás, törlés stb.) elleni szervezési és adminisztratív intézkedések, fizikai védelmi eszközök, műszaki és logikai megoldások összehangolt rendszere.

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

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 Társaság mindenkor hatályos Szervezeti és Működési Szabályzata szerinti azon szervezeti egység, amely az adott adatkezelést a Társaság, mint adatkezelő nevében és érdekében végzi.

Adattovábbítás: a személyes adat meghatározott harmadik személy (címzett) számára történő hozzáférhetővé tétele.

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

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

Adatvédelmi kapcsolattartó vagy Kapcsolattartó: az adatkezelést végző szervezeti egység vezetője által kijelölt személy, aki egy meghatározott adatkezelési cél vonatkozásában a Társaság adatkezelési nyilvántartásába bejegyzett adatbirtokos szervezeti egység kapcsolattartója. Abban az esetben, ha az adatkezelést végző szervezeti egység vezetője nem jelöl ki az adott adatkezelés vonatkozásában adatvédelmi kapcsolattartót, akkor a szervezeti egység vezetője minősül adatvédelmi kapcsolattartónak.

Érintett: bármely azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy.

Különleges adat: a személyes adatok különleges kategóriájába tartozó minden adat, azaz 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.

MÁV-csoport: A MÁV Zrt. és a teljeskörűen konszolidált gazdasági társaságai.

Személyes adat: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ.

Társaság: A MÁV Zrt. és MÁV-csoportba tartozó leányvállalat.

3.2 Rövidítések

- ASZE: Adatkezelő Szervezeti Egység
- ASZEV: Adatkezelő Szervezeti Egység Vezetője
- DPO: adatvédelmi tisztviselő
- EGT: Európai Gazdasági Térség
- GDPR: 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 irányelvhatályon kívül helyezéséről (általános adatvédelmi rendelet)
- Hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság
- IBSZ: a Társaság mindenkor hatályos Informatikai Biztonsági Szabályzata

3.3 Tárgyszavak

GDPR, személyes adat, adatkezelés, adatkezelő, adatfeldolgozó, adatvédelmi incidens.

4.0 AZ UTASÍTÁS LEÍRÁSA

4.1 A személyes adatok kezelésének általános szabályai

A Társaság nevében adatkezelést végző szervezeti egységek kötelesek az adatkezeléssel járó tevékenységeik teljes folyamatában – a folyamat tervezésétől annak befejezéséig – a jelen utasításban foglaltakat betartani.

Amennyiben a Társaság önálló adatkezelőként jár el, úgy az egyes adatkezelések jogszerűségéért harmadik személyek irányában a Társaság felelős.

Amennyiben a Társaság más adatkezelő adatfeldolgozójaként jár el, úgy az adatkezelés jogszerűségéért harmadik személyek irányában – az adatfeldolgozási szerződés rendelkezéseinek figyelembevételével – az adatkezelő felelős. Az adatkezelő és az adatfeldolgozó közötti felelősség megállapítására vonatkozó rendelkezéseket az adatfeldolgozási szerződésben kell rögzíteni. Amennyiben a Társaság adatfeldolgozóként végez adatkezelést, de a személyes adatok kezelésének célját – az adatkezelő utasításaival ellentétesen – önállóan határozza meg, túlterjeszkedik az adatfeldolgozási szerződésben foglalt jogain, úgy harmadik személyek irányában az adott túlterjeszkedéssel érintett adatok tekintetében önálló adatkezelőként felel.
Abban az esetben, ha a Társaság más adatkezelőkkel együtt közös adatkezelőként jár el, vagyis az adatkezelés célját és eszközeit más adatkezelőkkel közösen határozza meg, az adatkezelés részleteit – így különösen az adatkezelésért az egymás közötti (belső) felelősségüket – a GDPR 26. cikk (1) bekezdése szerinti közös adatkezelők közötti megállapodásban határozzák meg.

Jelen utasításban foglaltakat a mindenkor hatályos IBSZ előírásaival összhangban kell alkalmazni.

4.2 Az adatkezelésben közreműködők feladatai

4.2.1 Vezérigazgató/Ügyvezető

A Társaság vezérigazgatója/ügyvezetője jelöli ki az adatvédelmi tisztviselőt.

4.2.2 Adatvédelmi tisztviselő

A Társaság vezérigazgatója/ügyvezetője által kijelölt adatvédelmi tisztviselő az adatvédelemmel összefüggő feladatai ellátásával kapcsolatban utasításokat senkitől nem fogadhat el.Feladatainak ellátása során elősegíti a Társaságnak a személyes adatok kezelésére vonatkozó jogi előírásokban meghatározott kötelezettségeinek teljesítését, így különösen:

a) a személyes adatok kezelésére vonatkozó jogi előírásokról naprakész tájékoztatást nyújt az adatkezelési tevékenységet végzőknek,
b) tájékoztat és szakmai tanácsot ad a Társaság bármely munkavállalójánakaz adatvédelmi jogszabályoknak való megfelelés érdekében.
c) szakmai tanácsadással elősegíti és figyelemmel kíséri az adatvédelmi hatásvizsgálat lefolytatását,
d) együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és személyekkel, kapcsolatot tart a Hatósággal az előzetes konzultáció és a Hatóság által lefolytatott eljárások elősegítése érdekében,
e) vezeti az adatkezelési-, adatfeldolgozói-, adatvédelmi incidens és az érintetti kérelmek nyilvántartását.
f) kivizsgálja az adatvédelemmel kapcsolatos bejelentéseket,
g) ellenőrzi – Társaság információvédelemmel és IT biztonsággal kapcsolatos feladatokat ellátó szervezeti egységének bevonásával – a Társaság adatvédelmi és adatbiztonsági állapotát, szükség esetén javaslatokat fogalmaz meg annak javítására, az elvárt szint elérésére, fenntartására,
h) közreműködik a Társaság adatvédelmi oktatásával kapcsolatos feladatok ellátásában.
i) közreműködik a tudomására jutott adatvédelmi incidensek kivizsgálásában, szakmai tanácsot ad az incidens következményeinek elhárításához szükséges intézkedések meghatározásához. Amennyiben a GDPR és a jelen utasításban foglaltak szerint bejelentést kell tenni– az adatvédelmi incidens bekövetkezését bejelenti az Hatóságnak, és az adatkezelő szervezeti egység által adott információk alapján kialakítja szakmai álláspontját az érintettek értesítésének szükségességéről.

j) ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát a jogszabály nem határozza meg, az adatkezelés megkezdésétől számított legalább három (3) évente az adatkezelő szervezeti egység vezetőjével közösen a szükséges felülvizsgálatot elvégzi, és ellenőrzi, hogy a Társaság, mint adatkezelő által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e.

4.2.3 Adatkezelő szervezeti egység vezetője (ASZEV)

a) Új adatkezelés létrehozása során irányítja az adatkezeléssel összefüggő feladatok végrehajtását, különösen:
aa) kijelöli a Kapcsolattartót (szükséges szerint),
ab) felkéri az adatvédelmi tisztviselőt, hogy működjön közre az új adatkezeléshez kapcsolódó adatkezelési tájékoztató, – amennyiben az adatkezelési tevékenységhez szükséges – az adatfeldolgozási szerződés, és a Társaság adatkezelési tevékenységéhez kapcsolódó megállapodás előkészítésében.
b) Az adatkezelés megkezdése előtt legalább 3 (három) munkanappal az adatkezeléshez/feldolgozáshoz kapcsolódó valamennyi dokumentumot meg kell küldje az adatvédelmi tisztviselőnek.
c) Irányítja és ellenőrzi a szervezeti egység által kezelt személyes adatok védelmét.
d) Intézkedik a nem szabályszerű adatkezelési gyakorlat megszüntetéséről, az eset kivizsgálása érdekében értesíti az adatvédelmi tisztviselőt és – informatikai rendszer érintettsége esetén – amennyiben a Társaság valamely szervezeti egysége, akkor a rendszer üzleti tulajdonosát, valamint szükség esetén a Társaság információvédelemmel és IT biztonsággal kapcsolatos feladatokat ellátó szervezeti egységét.
e) Értesíti az adatvédelmi tisztviselőt az érintett által hozzá benyújtott kérelemről.

4.2.4 Adatvédelmi kapcsolattartó

a) Az adatvédelmi feladatok ellátása érdekében közvetlenül kapcsolatot tart az adatvédelmi tisztviselővel.
b) Az adatkezelésben bekövetkező változást haladéktalanul, de legalábba változást megelőző 3 (három) munkanapon belül – a szükséges előzmények és dokumentumok megküldésével – közli az adatvédelmi tisztviselővel.
c) Az adatkezelés kapcsolattartójaként figyelemmel kíséri a szervezeti egységénél folytatott adatkezeléseket, támogatást nyújt az adatkezelő szervezeti egység munkavállalói számára a jelen szabályzat és az adott adatkezelési tájékoztató előírásainak végrehajtásában.
d) A szervezeti egységnél bevezetésre tervezett új vagy módosítandó adatkezelési folyamat kialakítási szakaszában értesíti az adatvédelmi tisztviselőt, konzultál a megfelelő előkészítés érdekében.

e) Amennyiben az adatkezelés jogalapja a Táraság jogos érdeke, az adatvédelmi tisztviselő támogatása mellett – a szervezeti egység munkatársainak bevonásával – elkészíti az érdekmérlegelési tesztet.
f) Nem megfelelő adatkezelési gyakorlat észlelése esetén értesíti a szervezeti egység vezetőjét, szükség szerint előzetesen konzultál az adatvédelmi tisztviselővel.
g) Közreműködik az adatvédelmi ellenőrzési eljárás lefolytatásában, a felügyeleti hatóság megkeresése esetén részt vesz a kért információk összegyűjtésében, a tények feltárásában, és a választervezet elkészítésében.
h) Az adatkezeléshez kapcsolódó adatvédelmi incidenst indokolatlankésedelem nélkül, legkésőbb, az adatvédelmi incidensről történő tudomásszerzést követő 24 órán belül köteles bejelenteni az adatvédelmi tisztviselőnek, és egyidejüleg az incidenshez kapcsolódó valamennyi – rendelkezésre álló – dokumentumot megküldeni részére.
i) Részt vesz az adatkezeléssel kapcsolatos incidensek kivizsgálásában, kezelésében, szükség esetén az érintettek tájékoztatásának megszervezésében.
j) Érvényesíti az adatvédelmi előírásokat az adatkezelés teljes folyamatában, különös tekintettel az adatok törlésére.

4.2.5 Munkáltatói jogkörgyakorló

Jogosult a munkáltatói jogkör gyakorlása körébe tartozó munkavállalók munkavállalással összefüggő személyes adatait kezelni.

Intézkedik, hogy a munkavállaló a munkakörének, vagy munkaviszonyának bármely jogcímen a szervezetnél történő megszűnésekor a munkakör átadás-átvétele során - a számítógépén, a hálózati meghajtókon, külső adattárolón, valamint az elektronikus postafiókjában tárolt, illetve munkakörével összefüggésben papír alapon keletkezett - adattartalom átadása során a munkavállaló személyes adatai dokumentált módon törlésre kerüljenek, azon személyes adatok kivételével, amelyek vonatkozásában jogszabály az adatkezelés időtartamáról másként rendelkezik vagy a további adatkezelésre felhatalmazást ad. Az átadott adathordozókon kizárólag az átadást követően is szükséges, a Társaság tulajdonát képező anyagok maradhatnak. A személyes adatokat tartalmazó adatbázisokat a munkavállaló kell pontosan megjelölje, ennek elmaradásából eredően a Társasággal szemben követelést nem támaszthat.

4.2.6 A Társaság információbiztonságért felelős szervezeti egységének vezetője

a) közreműködik a személyes adatokkal kapcsolatos valamennyi információbiztonsági feladat ellátásában, amelyrea mindenkor hatályos IBSZ rendelkezéseiirányadók.
b) az adatvédelmi tisztviselővel együttműködve közreműködik az információbiztonságotérintő adatvédelmi incidensek kivizsgálásában.
c) az adatvédelmi tisztviselő felkérésére adatvédelmi auditban közreműködik.

d) az adatvédelmi tisztviselő felkérésére adatvédelmi incidens kivizsgálásában vesz részt.

4.3 A személyes adatok kezelésének kialakítása

Az adatvédelmi és adatbiztonsági intézkedések k, és jelen utasítás rendelkezéseinek betartása érdekében a személyes adatokat tartalmazó adatbázis kialakítása során a leendő adatkezelést végző szervezet vezetője - vagy az általa kijelölt személy (adatvédelmi kapcsolattartó) - irányításával legalább a következő intézkedéseket kell végrehajtani:

a) Annak a folyamatnak a meghatározása (végleges folyamatleírás), amelyhez az adatkezelés kapcsolódni fog.
b) Az adatkezelési koncepció megfogalmazása, legalább az alábbi információk meghatározásával:
ba) mi az adatkezelés célja,
bb) milyen személyes adatokat kívánnak kezelni,
bc) kik ismerhetik meg a személyes adatokat,
bd) meddig és hogyan akarják tárolni a személyes adatokat,
be) adattovábbítás esetén milyen módon kívánják biztosítani az adatbiztonságot.
c) Az adatkezelési tevékenységet végző szervezeti egység rögzítése.
d) Adatkezelést végző szervezeti egység vezetője kijelölhet adatvédelmi kapcsolattartót, ennek hiányában az adatkezelést végző szervezeti egység vezetője az adatvédelmi kapcsolattartó.
e) A Kapcsolattartó a tervezett adatkezelést megelőző legalább 5 (öt) munkanappal felveszi a kapcsolatot az adatvédelmi tisztviselővel vagy az általa kijelölt személlyel - a b) pontban megjelölt információk megadásával – az adatkezelési tájékoztató elkészítése, ésaz adatkezelés folyamatának, feltételeinek egyeztetése céljából. A felkérés az adatkezeléshez kapcsolódó adatfeldolgozási-, vagy adatkezelési megállapodás elkészítésére is kiterjedhet.
f) Abban az esetben, ha a tervezett adatkezelés jogalapja a Társaság jogos érdeke lesz, akkor az adatvédelmi tisztviselő köteles a Kapcsolattartót támogatni az érdekmérlegelési teszt elkészítésében.
g) Abban az esetben, ha az adatkezelési tevékenységet végző szervezeti egység önállóan, az adatvédelmi tisztviselő közreműködése nélkül készíti el az adatkezelési tájékoztatót, akkor az adatkezelés megkezdése előtt legalább 3 (három) munkanappal az adatkezelést be kell jelentense az adatvédelmi tisztviselőnekél, mellékelve kell az adatkezeléshez kapcsolódó valamennyi dokumentumot.
h) A Kapcsolattartó – szükség esetén az adatvédelmi tisztviselővel történő egyeztetést követően – gondoskodik arról, hogy az adatkezelés megkezdése előtt az érintettek – pl. egy kapcsolódó VIG utasítás mellékleteként/részeként, online és/vagy a helyben szokásos módon papír alapon – megismerhessék az

adatkezelési tájékoztatót, és az az adatkezelés időtartama alatt folyamatosan elérhető legyen az érintettek részére.

i) Az adatkezelés befejezését követően, az adatkezelési tájékoztatóban megjelölt határidőben a Kapcsolattartó köteles gondoskodni – az utasítás 1. sz. függeléke szerinti jegyzőkönyv kiállítása mellett – a személyes adatok törléséről.

4.4 Érintetti jogok gyakorlása

Amennyiben az érintett megkeresése érintetti kérelemnek minősül a GDPR alapján, az érintett kérelmére a vonatkozó információkat – az adatvédelmi tisztviselővel történő egyeztetést követőn – az érintettnek a Kapcsolattartó vagy az adatvédelmi tisztviselő köteles megadni az érintett kérelmének beérkezésével azonos módon (elektronikus vagy postai úton), illetve szóbeli tájékoztatás is adható (amennyiben személyazonosságát igazolta). Az érintetti jogok gyakorlása esetén – az azonosítást nem igénylő adatkezeléseket kivéve - az érintett – amennyiben az adatkezelő képviseletében eljáró személynek megalapozott kétsége van - köteles hitelt érdemlő módon igazolni a személyazonosságát.

Az érintetti jogok gyakorlása iránti kérelemnek nincsenek kötelező formai követelményei

Abban az esetben, ha az érintett közvetlenül a Kapcsolattartóhoz, vagy a Társasághoz fordul valamely érintetti jogának gyakorlásával kapcsolatban, akkor a Kapcsolattartó vagy annak a szervezeti egységnek a vezetője, ahova a kérelem érkezett, köteles legkésőbb a kérelem beérkezését követő 3 (három) munkanapon belül az adatvédelmi tisztviselőt értesíteni, és egyeztetni a válaszlevél tartalmát, illetve az esetlegesen szükséges intézkedéseket.

Az adatkezeléssel érintett szervezeti egység vezetője köteles gondoskodni arról, hogy – a jogszabályi feltételek fennálltakor – a Társaság határidőben teljesítse az érintett kérelmében foglaltakat.

Az érintett a jogainak gyakorlására irányuló kérelmét szóban (telefonon vagy személyesen) vagy képviselő útján írásban (postai úton vagy elektronikus úton) terjesztheti elő.

A kérelem akkor minősül beérkezettnek, amikor a szóban (telefonon vagy személyesen) benyújtott igény rögzítésre, az írásban, postai úton benyújtott igény az iratkezelési szabályok szerint érkeztetésre kerül, illetve amikor az elektronikus úton benyújtott igény a Társaság elektronikus postafiókjába beérkezik.

A kérelem teljesítése érdekében a Társaság adatkezelő szervezetének feladata meggyőződni arról, hogy a kérelmező olyan személynek minősül-e, akinek a személyes

adatát kezeli. Ennek megállapításához a kérelmezőt – a Társaság által kezelt személyes adatok alapján – azonosítani kell.

Az érintett kérelmét a Társaság indokolatlan késedelem nélkül, a kérelem beérkezésétől számított egy (1) hónapon belül köteles megválaszolni. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további kettő (2) hónappal meghosszabbítható. A határidő meghosszabbításáról a Társaság adatkezelő szervezeti egysége vagy az adatvédelmi tisztviselő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy (1) hónapon belül tájékoztatja az érintettet.

4.5 Az adattovábbítás szabályai

Személyes adatot a Társaság harmadik személy részére akkor továbbíthat, ha az adatok továbbítását jogszabály nem tiltja, a jogszabályban meghatározott feltételeket teljesíti és az adattovábbítás megfelelő jogalappal, célhoz kötötten, az IBSZ szerinti adatbiztonsági szabályok betartásával történik.

Amennyiben a Társaság az adatkezelő, az adattovábbításról a Társaság dönt. Ha a Társaság adatfeldolgozó, az adat(ok) továbbítására vonatkozó döntést nem hozhat, azt az adatkezelőnek kell meghoznia.

A személyes adatok továbbítását az adatot továbbító szervezeti egység köteles visszakereshető módon dokumentálni.

4.5.1. Külföldre történő adattovábbítással (nemzetközi adattovábbítással) kapcsolatos speciális szabályok

Az EGT tagállamba irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor. Harmadik országban (nem EGT tagállamban) adatkezelést folytató adatkezelő részére személyes adat főszabály szerint nem továbbítható, kivéve ha fennállnak a GDPR V. fejezetében rögzített feltételek. Harmadik országba (nem EGT tagállamba) történő adattovábbítás tervezésébe a Társaság adatot kezelő szervezeti egysége minden esetben köteles az adatvédelmi tisztviselőt bevonni.

4.6 Adatfeldolgozás

Az adatfeldolgozó által végzett adatkezelést az adatkezelő és az adatfeldolgozó közötti, a GDPR 28. cikke szerinti adatfeldolgozási megállapodásban kell rögzíteni. A megállapodásban szabályozni kell az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő és adatfeldolgozó jogait és kötelezettségeit.

Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, saját céljára adatfeldolgozást nem végezhet.

Az adatfeldolgozó a tudomására jutott személyes adatokat kizárólag az adatkezelő – elsősorban az adatfeldolgozási megállapodásban rögzített – rendelkezései szerint kezelheti, dolgozhatja fel, továbbá azokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni. Az adatfeldolgozó jogait és kötelezettségeit a GDPR, valamint az adatfeldolgozóval kötött adatfeldolgozási megállapodás határozza meg.

A Társaság adatfeldolgozási megállapodás megkötéséért felelős szervezeti egysége – nyilvántartásba vétel céljából – köteles a megkötött adatfeldolgozási megállapodást az adatvédelmi tisztviselő részére megküldeni a megállapodás aláírását követő 5 (öt) munkanapon belül.

A Társaság, mint az adatkezelő és a külső 3. fél, mint adatfeldolgozó közötti adatfeldolgozási megállapodás előkészítésébe minden esetben be kell vonni a Társaság adatvédelmi tisztviselőjét.

A Társaság adatkezelőként köteles olyan adatfeldolgozót igénybe venni, amely megfelelő garanciát nyújt az adatkezelés GDPR-ban foglalt követelményeinek való megfelelésre és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

4.7 Adatbiztonság

A Társaság a mindenkor hatályos IBSZ-ében foglaltak szerint védi a kezelésében lévő személyes adatokat a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint véletlen megsemmisülés és sérülés, továbbá hozzáférhetetlenné válás ellen és gondoskodik arról, hogy adatkezelési tevékenysége biztonságos legyen.

Az adatbiztonsági intézkedések meghatározása, megfelelőségük folyamatos figyelemmel kísérése a Társaság információbiztonságért felelős szervezeti egységének feladata. Ennek érdekében – a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint az érintett személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével – megteszi a szükséges technikai és szervezési intézkedéseket, amelyek az irányadó jogszabályok, adatvédelmi előírások érvényre juttatásához szükségesek, mind az elektronikus információs rendszerekben tárolt, mind a hagyományos, papír alapú adathordozókon tárolt adatállományok tekintetében.

4.7.1 Alapvető szervezési intézkedések

A személyes adatok védelmét szolgálja az ún. tiszta asztal és tiszta képernyő alkalmazása. Ezen intézkedések közé tartoznak az alábbiak.

a) A személyes adatokat tartalmazó papír alapú, valamint számítógépes adathordozók, hordozható számítógépek illetéktelen személy számára hozzáférhető módon, felügyelet nélkül nem hagyhatók.
b) A felügyelet nélkül hagyott iroda ajtaját minden esetben be kell zárni, oda illetéktelen személy bejutását egyéb technikai és szervezési intézkedésekkel meg kell akadályozni.
c) Személyes adatot tartalmazó információ nyomtatása során a nyomtató nem hagyható őrizetlenül. A nyomtatás folyamatában fellépő technikai akadály esetén gondoskodni kell a nyomtató memóriájának (feladatsorának) törléséről, illetve arról hogy később, az akadály elhárultával a nyomtató memóriájából kinyomtatásra kerülő dokumentum ne juthasson illetéktelen kezekbe.
d) Személyes adatokat tartalmazó, bekapcsolt állapotú számítógépet az iroda elhagyása esetén zárolni kell.

Az elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a különböző nyilvántartásokban tárolt adatok – amennyiben jogszabály vagy belső szabályozó nem teszi lehetővé – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők (profilalkotás).

4.7.2 Személyes adatokat tartalmazó iratok, adathordozók kezelése

Személyes adatokat tartalmazó iratok első sorban zárt borítékban továbbíthatók és azokon – szükség szerint – fel kell tüntetni a „Zártan kezelendő!” kezelési jelölést.

Személyes adatok elektronikus továbbítása során - a rendelkezésre álló lehetőségek felhasználásával (pl.: a Társaság által az IBSZ-ben foglaltakkal összhangban rendszeresített titkosítási módszerrel) – gondoskodni kell az adatok védett/zártan kezeléséről oly módon, hogy azokhoz kizárólag a megismerési jogosultsággal rendelkezők férhessenek hozzá.

A fentiek alól kivételt képeznek azok az elektronikus adattovábbítások, melyek tartalmi és formai elemeit jogszabály, vagy jogszabály felhatalmazása alapján a felügyeleti hatóság vagy személyes adatok továbbítását érintő és a Társaságra, mint félre irányadó szerződés, megállapodás írja elő, valamint a Társaság egyes humán szervezeti egységei közötti adattovábbítások, amennyiben megfelelően biztosított a munkavállalói személyes adatok illetéktelen hozzáférés elleni védelme.

4.7.3 Személyes adatokat tartalmazó informatikai eszközök átadása, elidegenítése

Informatikai, infokommunikációs eszköz (notebook, tablet, okostelefon stb.) más felhasználó számára történő átadása, értékesítése, selejtezése esetén – az IBSZ-ben foglaltak szerint – gondoskodni kell az eszközön található személyes adat(ok) teljes körű és vissza nem állítható módon történő törléséről.

4.7.4 Álnevesítés és anonimizálás

Álnevesítés esetén az azonosító mezőket egy vagy több mesterséges azonosítóval kell helyettesíteni. Az anonimizálás során az adatokon olyan visszafordíthatatlan átalakítást kell végrehajtani, amelynek eredményeként a korábban természetes személyhez kapcsolható adatok többé ne legyenek összekapcsolhatók a természetes személlyel.

A személyes adatok kezelése során – amennyiben erre mód és lehetőség van – előnyben kell részesíteni az anonimizálást. Amennyiben a személyes adatok kezelésére a továbbiakban még szükség van, az álnevesítés módszere választható. Ennek megvalósítása során a Társaságnak meg kell hoznia az érintett adatkezelés végrehajtásához szükséges technikai és szervezési intézkedéseket és biztosítania kell a személyes adatok egy adott érintetthez kapcsolásához szükséges további információk elkülönített tárolását. Ki kell jelölni továbbá a szervezeten belül azt a feljogosított személyt, aki a szükségessé váló összekapcsolást végrehajthatja.

A személyes adatok álnevesítése csökkentheti az érintettek számára a kockázatokat, valamint segíthet az adatkezelő szervezeti egységeknek és az adatfeldolgozóknak abban, hogy az adatvédelmi kötelezettségeiknek megfeleljenek.

4.7.5 Beépített és alapértelmezett adatvédelem

Az adatkezelési műveletek korai fázisainak tervezése során is olyan technikai és szervezési intézkedéseket kell a Társaságnak bevezetnie, amelyek kezdettől fogva szavatolják az érintett magánéletének védelmére irányuló adatvédelmi alapelvek érvényesülését (beépített adatvédelem).

Alapértelmezett módon biztosítja a Társaság azt, hogy a személyes adatok kezelésére a magánélet védelmének legszigorúbb tiszteletben tartásával kerüljön sor (pl. csak a szükséges adatok kezelése, rövid tárolási időszak, korlátozott hozzáférhetőség) és a személyes adatok ne válhassanak határozatlan számú személy számára hozzáférhetővé (alapértelmezett adatvédelem).

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 kockázatok figyelembevételével, a Társaság az alábbi megfelelő technikai és szervezési

intézkedéseket hajtja végre annak érdekében, hogy a Társaságnál a kockázat mértékének megfelelő szintű adatbiztonság garantált legyen:

a) a személyes adatok kezelésének minimálisra csökkentését.
b) a személyes adatok álnevesítését (személyazonosításra alkalmas anyagok mesterséges azonosítókkal való helyettesítése),
c) a személyes adatok titkosítását (üzenetek oly módon történő kódolása, hogy csak az arra felhatalmazottak tekinthessék meg),
d) a személyes adatok kezelésére használt rendszerek és szolgáltatások bizalmas jellegének folyamatos biztosítását, integritását, rendelkezésre állását és ellenálló képességét,
e) külső fizikai beavatkozásból vagy műszaki meghibásodásból eredő incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani,
f) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A személyes adatokhoz hozzáférők a mindenkor hatályos belső szabályozások (különösen a Társaság SZMSZ-ében foglaltak) szerint kizárólag az adatkezelő Társaság utasításának megfelelően kezelhetik az említett adatokat.

A Társaság különös figyelmet fordít az informatikai rendszereiben a szerepkörök kialakítására és a jogosultságmenedzsment megtervezésére, valamint a naplózás beállítására és a gyűjtött tevékenységi adatok ellenőrzésére.

4.8 A személyes adatok törlése

Amennyiben a Társaság kezelésében lévő személyes adat kezelésének időtartama letelt vagy az adatkezelés bármely egyéb a GDPR 17. cikke szerinti valamely okból megszűnik (pl. a Társaság adatkezeléshez fűződő célja szűnik meg) és jogszabály máshogy nem rendelkezik a Társaság törli, vagy anonimizálja az érintettre vonatkozó, az informatikai rendszereiben, valamint papír alapú dokumentációiban szereplő személyes adatokat.

Az adatok informatikai módszerrel történő tárolási módját úgy kell megválasztani, hogy abban a teljes körű és végleges törlés – az esetleg eltérő törlési határidőkre is tekintettel – a határidő lejártakor, illetve akkor, amikor az egyéb okból szükséges (pl.: az adatkezeléshez fűződő cél megszűnt és jogszabály máshogy nem rendelkezik), elvégezhető legyen. A törlésnek visszaállíthatatlannak és ellenőrizhetőnek kell lennie.

Elektronikus adathordozók (így különösen, de nem kizárólagosan merevlemezek, optikai adathordozók, mágneses adathordozók, nyomtatók, multifunkciós gépek háttértárai, adathordozók, SIM kártyák, mobileszközök, telefonok, tabletek, laptopok

stb.) esetében a Társaság mindenkor hatályos vonatkozó utasításában (pl IBSZ-ében) foglaltak szerint, az elektronikus adathordozók selejtezésére vonatkozó szabályok szerint kell gondoskodni a fizikai megsemmisítésről, illetve előzetesen az adatok biztonságos és visszaállíthatatlan törléséről.

A papír alapú adathordozókat iratmegsemmisítő berendezés segítségével, avagy azzal egyenértékű megoldással, illetve iratmegsemmisítésre szakosodott vállalkozó igénybevételével kell a személyes adatoktól megfosztani.

A személyes adatok törléséről a Kapcsolattartónak jegyzőkönyvet (1. sz. függelék) kell kiállítania, azt az aláírástól számított három (3) munkanapon belül tájékoztatásul meg kell küldeni az adatvédelmi tisztviselőnek.

Ha a személyes adat törlése az azt tartalmazó irat sérelme nélkül nem valósítható meg:

a) Amennyiben az irat megőrzéséhez a Társaság jogos érdeke fűződik, az iratot a Társaság mindenkor hatályos iratkezelési szabályzatában foglaltak szerinti időtartamig meg kell őrizni, törlési kérelem esetén az iratot zártan kell kezelni, erről az érintettet értesíteni szükséges, és az iratot a személyes adattal együtt az iratkezelési szabályban meghatározott időtartam lejártát követően meg kell semmisíteni.
b) Amennyiben az irat megőrzéséhez a Társaságnak nem fűződik jogos érdeke, az iratot a személyes adattal együtt meg kell semmisíteni. Az adatok törlése iránt minden esetben az adatkezelőnek a személyes adat kezelésében közreműködő szervezeti egységgel, valamint az informatikai rendszer rendszergazdájával együttműködésben kell intézkednie. Az adatkezelő informatikai rendszeréből a személyes adatot visszaállíthatatlanul törölni kell, és gondoskodni kell arról, hogy az informatikai rendszer archivált változatában is átvezetésre kerüljön a személyes adat törlése. A törlés megfelelőségét az informatikai rendszerért felelős személynek kell biztosítani.

Abban az esetben, ha a helyreállíthatatlan törlés informatikai okból nem kivitelezhető, az adatkezelő az adat logikai törlését hajtja végre. A logikai törlést megelőzően a személyes adatot olyan eltérő tartalomra kell lecserélni (anonimizálás), amely megakadályozza, hogy a személyes adathoz tartozó korábbi azonosítóval további adatok kapcsolatba hozhatók legyenek az érintettel. A papír alapú dokumentációk esetében azok iratkezelési szabályoknak megfelelően dokumentált megsemmisítéséről kell gondoskodni.

Amennyiben az adatok törlését jogszabály írja elő, de az az érintett jogos érdeke miatt ez nem lehetséges, a személyes adat kezelését (az adatot tartalmazó elektronikus vagy papír alapú dokumentációnak kizárólag tárolását végezve) korlátozni kell. Ez esetben az informatikai rendszerben tárolt adathoz, illetve dokumentumhoz csak az informatikai rendszer rendszergazdája, illetve az adatkezelő rendelkezhet hozzáféréssel. Papír alapú

dokumentációk esetén pedig a dokumentum őrzését zárható szekrényben kell megvalósítani.

4.9 Adatvédelmi incidens bekövetkezése esetén követendő eljárás

4.9.1 Adatvédelmi incidens

Az 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.

A Társaságnál tipikusan az alábbi adatvédelmi incidensek merülhetnek fel:

- A személyes adatok feletti rendelkezés elvesztése (pl.: személyes adatokat tartalmazó pendrive, notebook, mobiltelefon, illetve papír alapú dokumentumok elvesztése),
- az adatok véletlenül vagy jogellenesen törlésre kerülnek,
- személyes adatokat tartalmazó adatbázis sérülése (pl.: az informatikai rendszer egészének vagy egy részének használhatatlanná válása vírus vagy egyéb rosszindulatú szoftver által),
- személyazonossággal való visszaélés,
- az álnevesítés engedély nélküli feloldása,
- személyes adatok jogellenes nyilvánosságra hozatala (pl.: e-mail üzenet helytelen vagyis az eredeti címzettől eltérő – így különösen a Társaságon kívüli 3. félhez tartozó – címre történő elküldése)
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése.

Az adott cselekmény incidensként való minősítését nem befolyásolja, hogy azt szándékosan vagy véletlenül követték-e el.

4.9.2 Adatvédelmi incidens észlelése és kivizsgálása

Az adatvédelmi incidenst először észlelő munkavállaló köteles az adatvédelmi incidenst azonnal jelenteni (e-mailben, de súlyos, pl.: az érintettek nagy számát és/vagy a személyes adatok széles körét és/vagy a személyes adatok különleges kategóriájába tartozó személyes adatokat érintő incidens esetén telefonon is) a munkáltatói jogkörgyakorlójának, az adatkezelést végző szervezeti egység vezetőnek, és ezzel egyidejűleg az adatvédelmi tisztviselőnek, valamint a Társaság adatvédelmi incidens kapcsán rendelkezést tartalmazó egyéb utasításaiban (így különösen az IBSZ-ben, mobileszközökre vonatkozó utasításban) megjelölt további szervezeti egységeknek

A munkavállalónak a jelentésben röviden ismertetnie kell az észlelt esemény kapcsán rendelkezésére álló valamennyi információt, így különösen az adatvédelmi incidens

jellegét (azaz bekövetkezésének körülményeit), beleértve az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát. Ezzel párhuzamosan az adatkezelést végző szervezeti egység vezetője – az adatvédelmi tisztviselővel egyeztetve – haladéktalanul megtesz mindent annak érdekében, hogy az incidens következményeit enyhítse, a további károkat elhárítsa.

Adatvédelmi incidensre utaló információ esetén az adatkezelést végző szervezeti egység vezetőjének először azt kell megvizsgálnia, hogy bekövetkezett-e a biztonság olyan sérülése, amely a kezelt (pl.: továbbított, tárolt) személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Az incidens körülményeinek felderítéséhez és a következmények enyhítéséhez – amennyiben szükséges – bevonja a szükséges szakértelemmel rendelkező jogi és informatikai szakértőket is. Amennyiben nem állapítható meg az adatvédelmi incidens megtörténte, akkor azt kell vizsgálni, hogy a jelen utasítás helyett az IBSZ-t, vagy bármely más belső szabályzatot, esetleg egyéb jogszabályt sért-e a bekövetkezett incidens.

Amennyiben megállapításra került, hogy adatvédelmi incidens következett be, az adatvédelmi tisztviselő elektronikus úton (e-mail) tájékoztatja a Társaság vezérigazgatóját/ügyvezetőjét.

Adatvédelmi incidens bekövetkezése esetén kockázatértékelést kell végrehajtani, amelynek során az alábbi szempontokat kell figyelembe venni:

- az incidens bekövetkezésének időpontja,
- az incidens jellege,
- a személyes adatok típusa és mennyisége,
- az érintettek száma,
- az incidens lehetséges következményei az érintettek számára,
- az érintettek azonosíthatóságának egyszerűsége,
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések.

4.9.3 Az adatvédelmi incidens bejelentése a Hatóság részére

A bejelentési kötelezettség a tudomásszerzéstől, és nem az incidens bekövetkezésétől jön létre. Tudomásszerzésnek az tekinthető, amikor a munkavállaló (adatkezelő) észszerű mértékű bizonyossággal rendelkezik arról, hogy olyan esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet.
Az értesülésnek, illetve a belső vizsgálat megkezdésének időpontjában még nem kell úgy tekinteni, hogy az adatkezelőnek tudomása van az incidensről, ugyanakkor fontos azt kiemelni, hogy a belső vizsgálatot azonnal el kell kezdeni és 72 órán belül be kell

fejezni, tekintettel a GDPR alapján a Hatóság felé fennálló bejelentési kötelezettség határidejére. Amennyiben ezen időpontig nem tudott az adatkezelést végző szervezeti egység vezetője kellő bizonyosságot szerezni az incidensről, akkor vélelmezni szükséges az incidens bekövetkeztét és meg kell kezdeni az incidens bejelentését és kezelését, tekintettel arra, hogy az adatvédelmi incidens bejelentés bármikor visszavonható.

A bejelentés megtétele a Hatóság felé - az adatvédelmi tisztviselő útján - az adatkezelést végző szervezeti egység vezetőjének a kötelezettsége. Ha a bejelentés nem történik meg 72 órán belül, akkor közölni kell a késedelem igazolására szolgáló indokokat is.

Abban az esetben, ha a Társaság adatfeldolgozóként jár el, akkor az adatfeldolgozási megállapodásban meghatározott módon kell az adatvédelmi incidenssel kapcsolatos információkat az adatkezelőnek átadni. A Társaság, mint adatfeldolgozó - az adatfeldolgozási megállapodásban kijelölt személy útján, ennek hiányában a Kapcsolattartó útján - az adatvédelmi incidenst köteles az arról való tudomásszerzést követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek és legkésőbb ezzel egyidejűleg az adatvédelmi tisztviselőnek.

4.9.4 Az érintettek tájékoztatása

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Kapcsolattartó vagy az adatkezelést végző szervezeti egység vezetője késedelem nélkül tájékoztatja az érintettet/érintetteket az adatvédelmi incidensről.

A tájékoztatás tartalmát az érintettek értesítése előtt egyeztetésre meg kell küldeni az adatvédelmi tisztviselőnek.

A tájékoztatást közvetlenül az érintettnek kell megküldeni, kivéve, ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

A tájékoztatás során figyelemmel kell lenni arra, hogy a Társaság ne használja az incidensben esetleg érintett kommunikációs csatornákat addig, amíg azok biztonságáról meg nem bizonyosodott.

Ha az adatkezelést végző szervezeti egység vezetője amellett dönt, hogy az érintetteket nem tájékoztatja az incidensről, ezt a döntését megfelelően dokumentálni és indokolni szükséges, és erről az adatvédelmi tisztviselőt tájékoztatnia kell.

4.9.5. Az adatvédelmi incidens kezelésének lezárása

Az adatvédelmi incidens kivizsgálásáról szóló jelentést jóváhagyásra meg kell küldeni a Társaság vezérigazgatójának/ügyvezetőjének.

4.9.6 Adatvédelmi incidens nyilvántartás

Az adatvédelmi incidensekről szóló nyilvántartás vezetésért az adatvédelmi tisztviselő felel. A nyilvántartás legalább az alábbiakat tartalmazza:

a) Az érintett személyes adatok körét,
b) az adatvédelmi incidenssel érintettek körét és számát,
c) az adatvédelmi incidens időpontját, körülményeit, hatásait és
d) az elhárítására megtett intézkedéseket,
e) milyen indokok alapján döntöttek az adatvédelmi incidens bejelentéséről vagy annak mellőzéséről.

4.10 Nyilvántartások

Az adatkezelő szervezeti egység nyilvántartja az általa végzett adatkezelési folyamatok tekintetében alkalmazott valamennyi – hatályos és hatályát vesztett – adatkezelési tájékoztatót.

Az adatvédelmi tisztviselő köteles az adatkezelő szervezeti egység által részére megküldött hatályos adatkezelési tájékoztatók alapján adatkezelési nyilvántartást vezetni és abban javasolt rögzíteni különösen azt, hogy

- mely szervezeti egység felelős az adatkezelési tájékoztatóért,
- kik az adatkezelési tájékoztató érintettjei,
- mely utasítás mellékletét/függelékét képezi az adatkezelési tájékoztató,
- mi az adatkezelési tájékoztató kezdő (és ha van záró) időpontja,
- mi az adatkezelési tájékoztató alkalmazásának módja (online és/vagy papír alapú) és elérhetősége.

Az adatvédelmi tisztviselő köteles az általa vagy az adatkezelő szervezeti egység által készített és részére megküldött adatfeldolgozási megállapodások alapján adatfeldolgozási nyilvántartást vezetni és abban javasolt rögzíteni különösen

- az adatfeldolgozási megállapodás tárgyát és iktatószámát,
- az alapszerződés tárgyát és iktatószámát,
- a másik szerződő fél (adatkezelő vagy adatfeldolgozó) cégnevét és cégjegyzékszámát,
- a Társaság adatfeldolgozási megállapodás előkészítéséért felelős szervezeti egységét,
- az adatfeldolgozási megállapodás hatályát és

- a Társaság által esetlegesen igénybe vett további adatfeldolgozó cégnevét és cégjegyzékszámát.

Az adatvédelmi tisztviselő köteles a Társasághoz érkező érintetti kérelmekről nyilvántartást vezetni és abban javasolt rögzíteni különösen

- a kérelem kézhezvételének dátumát,
- a kérelem érkezésének módját,
- a kérelem beküldőjének nevét,
- az érintett nevét,
- a GDPR szerinti érintetti jogot,
- a kérelem tárgyát és tartalmát,
- a kérelem megválaszolásának határidejét,
- a kérelem megválaszolásának időpontját és módját,
- a kérelemre adott választ.

Az adatkezelési, illetve az adatfeldolgozási nyilvántartás tartalmára a GDPR előírásai az irányadóak.

4.11 Adatvédelmi 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 az adatkezelés megkezdését megelőzően adatvédelmi hatásvizsgálatot kell végeznie. Az adatvédelmi hatásvizsgálat lefolytatásába, valamint az elvégzett hatásvizsgálat felülvizsgálatába az adatvédelmi tisztviselőt be kell vonni.

5.0 HIVATKOZÁSOK, MÓDOSÍTÁSOK, HATÁLYON KÍVÜL HELYEZÉSEK

5.1 Hivatkozások

Az utasítás végrehajtása különösen az alábbi jogszabályok és egyéb szabályok figyelme vételével történik:

- 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),
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
- a Polgári törvénykönyvről szóló 2013. évi V. törvény,
- a munka törvénykönyvéről szóló 2012. évi I. törvény,
- a Társaság mindenkor hatályos Szervezeti és Működési Szabályzata,

- a Társaság mindenkor hatályos Iratkezelési Szabályzata,
- a Társaság mindenkor hatályos Informatikai biztonsági Szabályzata.

5.2 Hatályon kívül helyezések

Jelen utasítás hatályba lépésével egyidejűleg hatályát veszti

- a MÁV Zrt. adatvédelmi és adatbiztonsági szabályzatáról szóló 66/2021. (XII. 24. MÁV Ért. 23.) EVIG sz. utasítás,
- a MÁV Szolgáltató Központ Zrt. Adatvédelmi, Adatbiztosági és Adatvédelmi incidenskezelési szabályzatáról szóló 01/2019. VIG sz. utasítás.

6.0 HATÁLYBA LÉPTETŐ RENDELKEZÉS

Jelen utasítás a közzétételét követő napon lép hatályba.

7.0 MELLÉKLETEK, FÜGGELÉKEK JEGYZÉKE

Az utasítás függelékei a mindenkor hatályos normatív utasítások kiadásának rendjéről szóló utasítás szerint módosíthatók, egészíthetők ki. Az utasítás függelékei csak elektronikusan kerülnek közzétételre. Az utasítás hatályos függelékei a Társaság utasítástárában érhetők el.

7.1 Mellékletek

Jelen utasításnak nincsenek mellékletei.

7.2. Függelékek

1. sz. függelék: Adattörlési jegyzőkönyv (minta)
2. sz. függelék: Személyes adatok kezelésének kialakítása – folyamatábra
3. sz. függelék: Adatvédelmi incidenskezelés - folyamatábra