66/2021. (XII.24. MÁV Ért. 23.) EVIG sz. utasítás
a MÁV Zrt. adatvédelmi és adatbiztonsági szabályzata

1.0 AZ UTASÍTÁS CÉLJA

Jelen utasítás célja, hogy meghatározza a MÁV Zrt. (a továbbiakban: „Társaság”) 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 Társaság valamennyi munkavállalójára, továbbá a munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott személyekre.

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 Megfelelés támogatás vezető felel.

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;

Adatvédelmi 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.

Adatvédelmi tisztviselő (DPO: Data protection officer): az Elnök-vezérigazgató által kijelölt személy, az utasítás kiadásakor a Megfelelés támogatás vezető.

Anonimizálás: az érintettről 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.

Automatizált döntéshozatal: az a képesség, hogy technológiai eszközök segítségével, emberi beavatkozás nélkül hoznak döntéseket.

Azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

Érintett: bármely információ alapján azonosított vagy azonosítható természetes személy.

IBSZ: a MÁV Zrt. Informatikai biztonsági szabályzata (a jelen utasítás kiadásakor a 48/2020. (III.06. MÁV Ért. 9.) EVIG sz. utasítás).

Személyes adat: az érintettre vonatkozó bármely információ.

Üzleti tulajdonos: az a vezető, aki egy adott informatikai rendszert érintően jogosult a fejlesztésekkel, beszerzésekkel, az adatkezelést támogató informatikai rendszer használatával és karbantartásával kapcsolatos döntéseket meghozni (részletes definíciója az IBSZ-ben található).

4.0 AZ UTASÍTÁS LEÍRÁSA

4.1 Az adatkezelésben közreműködők feladatai

4.1.1 Elnök-vezérigazgató

A Társaság Elnök-vezérigazgatója jelöli ki az adatvédelmi tisztviselőt.

4.1.2. Megfelelés támogatás vezető

a) Felkérés esetén gondoskodik az adatkezelési tájékoztató elkészítéséről, illetve az adatfeldolgozási szerződés, továbbá az adott adatkezelési tevékenységéhez kapcsolódó megállapodás/szerződés elkészítéséről.
b) Ellátja az adatvédelmi tisztviselő feladatait.
c) Ellenőrzi a jogszabályoknak és a Társaság személyes adatok védelmével kapcsolatos szabályzatainak, adatkezelési tájékoztatóinak való megfelelést.
d) Kérésre tanácsot ad az adatvédelmi incidensről szóló bejelentés és ahhoz kapcsolódó tájékoztatás szükségessége, valamint az adatvédelmi hatásvizsgálat tekintetében, nyomon követi azok végrehajtását, illetve támogatja az adatkezelőt, illetve az adatfeldolgozót a felügyeleti hatósággal történő konzultáció lefolytatásában.
e) Az adatkezelést végző szervezeti egység vezetőjével együttműködve válaszol az adatvédelmi kérdésekben a hozzá intézett megkeresésére.
f) Gondoskodik az érintettek jogai érvényesítése érdekében hozzá benyújtott megkeresések kezeléséről.

g) Gondoskodik az adatkezelési-, adatfeldolgozói-, adatvédelmi incidens és az érintetti kérelmek nyilvántartás vezetéséről.
h) Részt vesz az adatvédelemmel összefüggően bekövetkezett incidensek kivizsgálásában.

4.1.3 Adatkezelést végző szervezeti egység vezetője

a) Új adatkezelés létrehozása során irányítja az adatkezeléssel összefüggő feladatok végrehajtását, különösen:
aa) kijelöli az adatvédelmi kapcsolattartót (amennyiben szükségesnek tartja),
ab) közvetlenül vagy az adatvédelmi kapcsolattartó útján felkéri az adatvédelmi tisztviselőt, hogy az új adatkezeléshez kapcsolódó adatkezelési tájékoztatót, illetve – amennyiben az adatkezelési tevékenységhez szükséges – az adatfeldolgozási szerződést, továbbá a Társaság adatkezelési tevékenységéhez kapcsolódó megállapodás/szerződés készítse el.
b) Abban az esetben, ha az adatkezelési tájékoztatót vagy az adatfeldolgozási szerződést nem az adatvédelmi tisztviselő készíti el, akkor – legkésőbb az adatkezelés megkezdése előtt 3 (három) munkanappal – köteles gondoskodni arról, hogy a szervezeti egység által végzett adatkezelés adatkezelési tájékoztatóját, illetve – amennyiben szükséges – adatfeldolgozási megállapodását, és az adatkezeléshez kapcsolódó valamennyi dokumentum az adatvédelmi tisztviselőnek megküldésre kerüljön.
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 – a rendszer üzleti tulajdonosát.
e) Értesíti az adatvédelmi tisztviselőt az érintett által hozzá benyújtott kérelemről.

4.1.4 Adatvédelmi kapcsolattartó

a) Az adatvédelmi feladatok ellátása érdekében közvetlenül kapcsolatot tart az adatvédelmi tisztviselővel.
b) Az adatkezelésben bekövetkező változást haladéktalanul, de legkésőbb a változást megelőző 3 (három) munkanapon belül 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 koncepció kialakítási szakaszában értesíti az adatvédelmi tisztviselőt, konzultál a megfelelő előkészítés érdekében,
e) A nem megfelelő adatkezelési gyakorlat észlelése esetén értesíti a szervezeti egység vezetőjét, szükség szerint előzetesen konzultál az adatvédelmi tisztviselővel.
f) Közreműködik az adatvédelmi ellenőrzési eljárás lefolytatásában, illetve a felügyeleti hatóság megkeresése esetén részt vesz a tények feltárásában, a kért információk összegyűjtésében és a választervezet elkészítésében.
g) Az adatkezeléshez kapcsolódó adatvédelmi incidenst indokolatlan késedelem nélkül, de legkésőbb 48 órával azután, hogy az adatvédelmi incidens a tudomására jutott köteles bejelenteni az adatvédelmi tisztviselőnek, és az incidenshez kapcsolódó valamennyi bizonyítékot megküldeni az adatvédelmi tisztviselőnek.

h) Részt vesz az adatkezeléssel kapcsolatban bekövetkezett incidensek kivizsgálásában, annak kezelésében, szükség esetén az érintettek tájékoztatásának megszervezésében.
i) Érvényesíti az adatvédelmi előírásokat az adatkezelés teljes folyamatában, különösen az adatok törlésére vonatkozóan.

4.1.5 Munkáltatói jogkörgyakorló

Jogosult a jogkörgyakorlása körébe tartozó munkavállalók munkavállalásukkal összefüggő személyes adatait kezelni.

Intézkedik, hogy az adott munkavállaló a munkakör-, szervezetváltáskor vagy munkaviszony megszűnésekor/megszüntetésekor a munkakör átadás-átvétele során a számítógépén, a hálózati meghajtókon, külső adattárolón, valamint az elektronikus postafiókjában tárolt, illetve munkakörével összefüggésben papír alapon keletkezett adatai átadása során az átadó munkavállaló személyes adatai dokumentált módon – a 6. számú melléklet munkavállaló általi kitöltésével – törlésre kerüljenek. Az átadott adathordozókon kizárólag az átadást követően is szükséges, a Társaság tulajdonát képező anyagok maradhatnak, azonban a személyes adatokat tartalmazó adatbázisokat a munkavállalónak kell pontosan megjelölnie, ennek elmaradásából eredően semmiféle követeléssel nem élhet a Társasággal szemben.

4.2 A személyes adatok kezelésének kialakítása

Az adatvédelmi és adatbiztonsági intézkedések betartásának, valamint a jelen utasítás rendelkezéseinek érvényesülése érdekében a személyes adatokat érintő adatkezelések, a személyes adatokat tartalmazó adatbázis kialakítása során a leendő adatkezelést végző szervezet vezetőjének vagy az általa kijelölt személy (adatvédelmi kapcsolattartó) irányításával legalább a következő intézkedéseket kell végrehajtani:

a) Annak a folyamatnak a végleges meghatározása (a folyamatleírás lezárása), amelyhez az adatkezelés majd kapcsolódni fog.
b) Az adatkezelés koncepciójának 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 kijelölése.
d) Adatkezelést végző szervezeti egység vezetője kijelölheti az adatvédelmi kapcsolattartót. Kijelölés hiányában az adatkezelést végző szervezeti egység vezetője lesz az adatvédelmi kapcsolattartó (a továbbiakban: „**Kapcsolattartó**”).
e) A Kapcsolattartó legkésőbb a tervezett adatkezelést megelőző 5 (öt) munkanappal korábban felveszi a kapcsolatot a Megfelelés támogatás szervezeti egységgel, hogy – legalább a b) pontban megjelölt információk megadásával – az adatkezeléshez szükséges adatkezelési tájékoztatót készítse, illetve egyeztessék az adatkezelés folyamatát, feltételeit. A felkérés az adatkezeléshez kapcsolódó adatfeldolgozási-, vagy adatkezelési megállapodás elkészítésére is kiterjedhet.

f) Abban az esetben, ha az adatkezelés jogalapja a MÁV Zrt. jogos érdeke lesz, akkor a Megfelelés támogatás szervezeti egység köteles a Kapcsolattartót támogatni az érdekmérlegelési teszt elkészítésében.
g) Abban az esetben, ha az adatkezelési tevékenységet végző szervezeti egység készíti el az adatkezelési tájékoztatót, akkor legkésőbb az adatkezelés megkezdése előtt 3 (három) munkanappal az adatkezelést be kell jelentenie az adatvédelmi tisztviselőnél, és mellékelni kell az adatkezeléshez kapcsolódó valamennyi dokumentumot.
h) A Kapcsolattartó gondoskodik arról, hogy az adatkezelés megkezdése előtt az érintettek megismerhessék az adatkezelési tájékoztatót, és az adatkezelés időtartama alatt folyamatosan elérhető legyen az érintettek részére.
i) Az adatkezelés befejezését követően, az adatkezelési tájékoztatóban megjelölt határidőben a Kapcsolattartó köteles gondoskodni – jegyzőkönyv kiállítása mellett – személyes adatok törléséről.

4.3 Az érintetti jogok gyakorlása

Az érintett kérelmére a vonatkozó információkat a Kapcsolattartó köteles megadni olyan módon, ahogy az érintett kérelme beérkezett (elektronikus vagy postai úton), illetve szóbeli tájékoztatás is adható. Az érintetti jogok gyakorlása esetén az érintett köteles hitelt érdemlő módon igazolni a személyazonosságát.

Az érintetti jogok gyakorlása iránti kérelem formanyomtatványa, és az ahhoz kapcsolódó adatkezelési tájékoztató a jelen utasítás mellékletét képezi.

Abban az esetben, ha valamely 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 indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezését követő 3 (három) munkanapon belül az adatvédelmi tisztviselőt értesíteni, és egyeztetni a válaszlevél tartalmat, illetve az esetlegesen szükséges intézkedéseket.

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

4.4 Adatvédelmi incidens bekövetkezése esetén követendő eljárás

4.4.1 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 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.

4.4.2 Adatvédelmi incidens észlelése és kivizsgálása

Az adatvédelmi incidenst először észlelő munkavállaló köteles az adatvédelmi incidenst azonnal jelenteni (e-mailben, de súlyos incidens esetén telefonon is) az adatkezelést végző szervezeti egység vezetőnek, és ezzel egyidejűleg az adatvédelmi tisztviselőnek.

A munkavállalónak a jelentésben röviden ismertetnie kell az adatvédelmi incidens jellegét, beleértve az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriát 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.

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

a) az incidens bekövetkezésének időpontja,
b) az incidens jellege,
c) a személyes adatok típusa és mennyisége,
d) az érintettek száma,
e) az incidens lehetséges következményei az érintettek számára,
f) az érintettek azonosíthatóságának egyszerűsége,
g) az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések.

4.4.3. Az adatvédelmi incidens bejelentése

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. 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 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.

4.4.4 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 indokolatlan 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, ettől függetlenül ezt a döntését megfelelően dokumentálni és indokolni szükséges, és erről az adatvédelmi tisztviselőt tájékoztatnia kell.

4.4.5 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.

4.5 Egyéb nyilvántartások vezetése

Az adatvédelmi tisztviselő köteles az általa készített és a részére megküldött adatkezelési tájékoztatók alapján adatkezelési nyilvántartást, illetve az általa készített és a részére megküldött adatfeldolgozási megállapodások alapján adatfeldolgozási nyilvántartást vezetni. Az adatkezelési, illetve az adatfeldolgozási nyilvántartás tartalmára a GDPR előírásai az irányadóak.

Az adatvédelmi tisztviselő köteles a beérkezett érintetti kérelmekről nyilvántartást vezetni, mely legalább a következő adatokat tartalmazza: kérelem nyilvántartási száma, a kérelem beérkezésének ideje, kérelem tárgya, válasz kiküldésének időpontja, intézkedés kellet-e tenni.

4.6 Adatbiztonsági intézkedések

A **s**zemélyes adatok megfelelő kezelése érdekében a Társaság valamennyi munkavállalója köteles mind a papír alapú dokumentumok, mind a digitális adathordozók fizikai hozzáférés védelméről gondoskodni. Ennek betartását a munkáltató jogkörgyakorló és a Megfelelés támogatás szervezeti egység alkalomszerűen ellenőrizheti.

4.6.1 Alapvető szervezési intézkedések

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

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 arról, 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 számítógép felhasználója a munkaszoba ideiglenes elhagyása esetén zárolja a számítógépét.

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).

4.6.2 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 gondoskodni kell az adatok védett kezeléséről oly módon, hogy azokhoz kizárólag a megismerési jogosultsággal rendelkezők férhessenek hozzá – elektronikus feldolgozás, továbbítás esetén, a rendelkezésre álló lehetőségek felhasználásával – technikai védelemmel (pl. a társaság által rendszeresített titkosítási módszerrel) is biztosítani kell.

Kivételt képeznek azok az elektronikus adattovábbítások, melyek tartalmi és formai elemeit jogszabály, vagy jogszabály felhatalmazása alapján a felügyeleti hatóság írja elő, valamint a Humánerőforrás vezérigazgató-helyettesi szervezet belső szervezeti egységei közötti adattovábbítás, amennyiben megfelelően biztosított a munkavállalói személyes adatok illetéktelen hozzáférés elleni védelme.

4.6.3 Személyes adatokat tartalmazó informatikai eszközök átadása, elidegenítése

Informatikai, infokommunikációs eszköz (notebook, tablet, okostelefon stb.) más felhasználó számára történő átadása, értékesítése, selejtezése esetén gondoskodni kell az eszközön található személyes adatok törléséről (lásd: IBSZ rendelkezései).

4.6.4 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 össze 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 az adatkezelőnek 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.

Mivel az anonimizálás következtében az adat elveszíti a személyes adat jellegét, ezért az ilyen adatra már nem kell alkalmazni a személyes adatok védelmére vonatkozó előírásokat. Erre tekintettel az anonimizáló algoritmust oly módon kell megalkotni,

hogy a megmaradó adatból az eredeti személyes adat ne többé már ne legyen visszaállítható, azaz az érintett se közvetlenül se közvetetten ne váljon azonosíthatóvá, még további adatok hozzáadásával sem.

Az álnevesített adatok azonban továbbra is a személyes adatok védelmére vonatkozó szabályok hatókörében maradnak. Az álnevesítés lényege, hogy a személyes adatok védelme során ez az adatok magas szintű védelmének egyik eszköze.

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.

4.6.5 Beépített és alapértelmezett adatvédelem

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

Alapértelmezett módon kell biztosítani 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), hogy alapértelmezett módon a személyes adatok ne válhassanak határozatlan számú személy számára hozzáférhetővé (alapértelmezett adatvédelem).

Erre tekintettel 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, megfelelő technikai és szervezési intézkedéseket kell végrehajtani annak érdekében, hogy az a kockázat mértékének megfelelő szintű adatbiztonság garantált legyen, ideértve:

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.

Biztosítani kell, hogy a személyes adatokhoz hozzáférők kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat. Különös figyelemmel kell lenni az informatikai rendszerben a szerepkörök kialakítására és a

jogosultságmenedzsment megtervezésére, valamint a naplózás beállítására és a gyűjtött tevékenységi adatok ellenőrzésére.

4.6.6 A személyes adatok törlése

Az adatok informatikai módszerrel történő tárolási módját úgy kell megválasztani, hogy abban a törlés – az esetleg eltérő törlési határidőkre is tekintettel – a határidő lejártakor, illetve akkor, amikor az egyéb okból szükséges, elvégezhető legyen. A törlésnek visszaállíthatatlannak és ellenőrizhetőnek kell lennie.

Elektronikus adathordozók (merevlemezek, optikai adathordozók, mágneses adathordozók, nyomtatók, multifunkciós gépek háttértárai, adathordozók, SIM kártyák, mobileszközök, telefonok, tabletek, laptopok stb.) esetében az IBSZ elektronikus adathordozók selejtezésére vonatkozó szabályai 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 jegyzőkönyvet kell kiállítani, amit az aláírásától számított három munkanapon belül tájékoztatásul meg kell küldeni az adatvédelmi tisztviselőnek.

Amennyiben a személyes adat kezeléséhez fűződő cél megszűnt és jogszabály máshogy nem rendelkezik az adatkezelő törli, vagy anonimizálja az érintettre vonatkozó, az informatikai rendszereiben, valamint papír alapú dokumentációiban szereplő személyes adatokat.

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

a) Amennyiben az irat megőrzéséhez az adatkezelő, vagy harmadik személy jogos érdeke fűződik, az iratot az adatkezelőnek az iratkezelési szabályok szerinti időtartamig meg kell őriznie, törlési kérelem esetén az iratot zártan kell kezelnie, 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 az adatkezelőnek és harmadik személynek sem 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, amennyiben lehetséges, visszaállíthatatlanul törölni kell, továbbá gondoskodnia kell arról, hogy az informatikai rendszer archivált változatában is átvezetésre kerüljön a személyes adat törlése. A törlés megfelelőségét az informatikai rendszerért felelős személynek kell biztosítania.

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.

5.0 HIVATKOZÁSOK, MÓDOSÍTÁSOK, HATÁLYON KÍVÜL HELYEZÉSEK

5.1 Hivatkozások

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

- 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 szóló Európai Parlament és a Tanács (EU) 2016/679 Rendelet (GDPR),
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
- a MÁV Zrt. Szervezeti és Működési Szabályzatának és Döntési és Hatásköri Listájának hatályba léptetéséről szóló 32/2021. (VI.25. MÁV Ért. 10.) EVIG sz. utasítás.
- a MÁV Zrt. Informatikai biztonsági szabályzatáról szóló 48/2020. (III.06. MÁV Ért. 9.) EVIG sz. utasítás.

5.2 Hatályon kívül helyezések

Ezen utasítással hatályát veszti a MÁV Zrt. adatvédelmi és adatbiztonsági szabályzatáról szóló 54/2020. (III. 13. MÁV Ért. 10.) EVIG számú utasítás.

6.0 HATÁLYBA LÉPTETŐ RENDELKEZÉS

Jelen utasítás a MÁV Értesítőben történő közzétételt követő napon lép hatályba.

7.0 MELLÉKLETEK JEGYZÉKE

1. számú melléklet: Adatkezelési bejelentőlap
2. számú melléklet: Kérelem érintetti jogok gyakorlása iránt *(Nyomtatvány)*
3. számú melléklet: Adatkezelési tájékoztató – Érintetti joggyakorlás
4. számú melléklet: Adattörlési jegyzőkönyv *(Mintadokumentum)*

5. számú melléklet: Érdekmérlegelési teszt
6. számú melléklet: Nyilatkozat – Informatikai eszközök adattartalmáról
7/a. számú melléklet: Személyes adatkezelés kialakításának folyamata (Elektronikus közzététel)
7/b. számú melléklet: Adatvédelmi incidens kezelésének folyamata (Elektronikus közzététel)

Dr. Homolya Róbert
elnök-vezérigazgató