

24/2014. (II. 12. MÁV-START Ért. 9.) sz. vezérigazgatói utasítás a MÁV-START Zrt. Adatvédelmi Szabályzata

1.0 AZ UTASÍTÁS CÉLJA

Az utasítás célja az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) előírásai végrehajtásának szabályozása a MÁV-START Zrt.-nél (a továbbiakban: Társaság), különösen a helyi adatkezelések elveinek és rendjének meghatározása, a személyes adatok felhasználási, továbbítási és védelmi szabályainak rögzítése.

2.0. HATÁLY ÉS FELELŐSSÉG MEGHATÁROZÁSA

2.1. Az utasítás hatálya

Az utasítás hatálya a Társaságnál folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira vonatkozik, valamint a Társasággal szerződéses jogviszonyban álló természetes és jogi személyre, jogi személyiséggel nem rendelkező szervezetre, a velük kötött szerződésben, illetve titoktartási nyilatkozatban rögzített mértékben. Az utasítást a számítógéppel, valamint a manuális módon végzett adatkezelésre és adatfeldolgozásra egyaránt alkalmazni kell.

2.2. Az utasítás kidolgozásáért és karbantartásáért felelős

A szabályzat kidolgozásáért és karbantartásáért a Társaság biztonsági vezetője felelős.

3.0. FOGALMAK MEGHATÁROZÁSA

3.1. Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek, vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

3.2. Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

3.3. Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása, megsemmisítése és tönkremenetele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere (a védelem tárgya az adat).

3.4. Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől feltéve hogy a technikai feladatot az adatokon végzik.

3.5. Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – személyes adatok feldolgozását végzi.

3.6. Adathordozó: a papír és azok a számítógépes alkatrészek, eszközök, amelyekre a munkához szükséges adatokat menteni, tárolni lehet, illetve a hordozható változataikkal gép-gép között adatot lehet cserélni, például:

- mágneses elven működő egységek (pl.: FDD, HDD, IBM Microdrive),
- optikai adattárolás elvén működő adathordozók (pl.: CD, DVD, Blu-ray Disc (BD)),
- memóriakártyák (pl.: Smart Media, Compact Flash, SDHC),
- USB, soros, IRDA portra csatlakoztatható eszközök (pl.: pen-drive, okostelefon, fényképezőgép, zenelejátszók, videokamerák).

3.7. Adatkezelés: az alkalmazott eljárástól függetlenül a személyes adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is.

3.8. Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

3.9. Adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

3.10. Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

3.11. Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

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

3.13. Adatvédelem: a személyes adatok kezelésével kapcsolatos jogi szabályozás, ami az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik (a védelem a személyre, az ún. adatalanyra irányul).

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

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

3.16. EGT-állam: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;

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

3.18. Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely

nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.

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

3.20. Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

3.21. Közvetlen vezető: aki a Társaság által biztosított számítógépet, e-mail címet használó munkatárs munkáját irányítja.

3.22. Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésre, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

3.23. Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

3.24. Különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselési szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

3.25. Magánterület: a közforgalom elől elzárt terület.

3.26. Munkáltatói jogkört gyakorló vezető: aki a munkaviszonyra vonatkozó rendelkezések keretei között a Társaság által alkalmazott munkatársat irányít.

3.27. "Nem nyilvános!" kezelési jelölés: a személyes adatot tartalmazó dokumentum általános jelölése; az így jelölt dokumentum az érintett életében csak akkor hozható nyilvánosságra, ha azt törvény elrendeli, vagy ahhoz az érintett hozzájárult.

3.28. Nyilvános magánterület: a magánterületnek a közforgalom számára a tulajdonos, illetve használó által megnyitott és kijelölt része, illetve azon magánterület, amelyet azonos feltételekkel bárki használhat.

3.29. Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

3.30. Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adathól levonható, az érintettre vonatkozó következtetés.

3.31. Személyesadat-nyilvántartó rendszer: személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető (pl. ANDOC, IHIR, e-Ticket alkalmazás).

3.32. Személyes használatú számítógép: az adott személy állandó jelleggel dolgozik a gépen, továbbá csak az adott személynek és rendszergazdának van a géphez hozzáférési jogosultsága.

3.33. Távközlési/informatikai eszköz üzemeltető: az a – rendszerint külső cég, vállalat, amely ezeket az eszközöket a vele kötött szerződés alapján a Társaságnál telepíti, javítja, karbantartja stb., és amelyet a szerződésben a Társaság biztonsági szabályainak a betartására köteleztek.

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

3.35. Ügyfél: az utas, az utazás előkészítése, helyfoglalás, stb. érdekében a nyilvános on-line rendszereken (e-Ticket, ELVIRA, stb.) a

Társasághoz forduló, a Társaság ügyfél-szolgálatától információt kérő vagy ott bejelentést, panaszt tevő személy, továbbá a Társaság által üzleti ajánlattal megkeresett, és a kedvezményes utazásra jogosító igazolvánnyal ellátott személy.

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

3.37. Területi biztonsági szakértő: a Biztonság szervezetébe tartozó munkavállaló, aki területi szerveknél látja el a biztonsági feladatokat.

3.38. Üzleti tulajdonos: az információs rendszer üzleti tulajdonosa az a – lehetőleg – magasabb beosztású vezető, akinek jogában áll a rendszer fejlesztésével, beszerzésével, használatával és karbantartásával kapcsolatos döntéseket meghozni. Célszerűen az a szervezeti egységi vezető, akihez az adott rendszer felhasználóinak többsége tartozik. Az informatikai biztonsági szempontok szerint értelmezett „tulajdonos” felelőssége kiterjed az adott rendszer informatikai termékeit, illetve szolgáltatásait érintő hagyományos és számítógépes feldolgozás biztonsága érdekében hozott valamennyi intézkedésre. Ő a rendszer biztonsági kockázatainak kezelője, de megbízottakat nevezhet ki, akik a nevében eljárnak. Ugyanazon személy egyszerre több rendszernek is lehet az üzleti tulajdonosa. A MÁV csoport által közösen használt rendszerek esetében (pl. GIR, IHIR) az üzleti tulajdonos felelőssége csak a Társaság által használt modulra terjed ki, feladatai e körre szűkítve értelmezettek.

3.39. Felhő alapú rendszerek: a szolgáltatásokat nem egy dedikált hardver-eszközön üzemeltetik, hanem a szolgáltató eszközein elosztva, a szolgáltatás üzemeltetési részleteit a felhasználótól elrejtve. Ezeket a szolgáltatásokat a felhasználók hálózaton keresztül érhetik el, publikus felhő esetében az Interneten keresztül, privát felhő esetében a helyi hálózaton vagy az Interneten.

3.40. QR kód: kétdimenziós vonalkód (pontkód), az angol *Quick Response* (=gyors válasz) rövidítése. A QR-kód nyílt szabványú, a specifikációi nyilvánosak, ISO/IEC 18004 jelzettel nemzetközi szabvánnyá vált, amit 2006-ban kiegészítettek. Bármilyen irányból olvasható, nem kell törődni a kód helyes tájolásával. A QR-kódokban nyílt és rejtett szövegek, Internetes címek, azok leolvasásakor azonnal futtatható programsorok, utasítások, stb. helyezhetők el.

4.0 AZ UTASÍTÁS LEÍRÁSA

4.1. A társaság adatvédelmi alapelvei

4.1.1 Az adatkezelés szabályai

Személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt törvény, vagy törvényi felhatalmazása alapján, az abban meghatározott körben, helyi önkormányzat elrendeli. Különleges adat akkor kezelhető, ha az adatkezeléshez az érintett írásban hozzájárul, vagy törvény elrendeli.

A személyes adatok védelméhez fűződő jogot és az érintett személyiségi jogait – ha törvény kivételt nem tesz – az adatkezeléshez fűződő más érdekek, ideértve a közérdekű adatok nyilvánosságát is, nem sérthetik.

A Társaság adatkezelési szabályait összefoglaló tájékoztatást kell elhelyezni a Társaság internetes honlapján, továbbá minden olyan elektronikus, vagy papír alapú dokumentumon (pl. kedvezményes utazási kártya igénylőlapja, Utasleadási lap), amelyen ügyfelek személyes adatait a Társaság bekéri.

4.1.2. Az adatkezelés célhoz kötöttsége

Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében szabad. Az adatkezelésnek minden szakaszában meg kell felelnie ennek a követelménynek.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, és a cél elérésére alkalmas. Az adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

Az érintettel az adat felvétele előtt közölni kell, hogy az adatszolgáltatás önkéntes vagy kötelező. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő

jogszabályt is. Az érintettet – egyértelműen és részletesen – tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Az ügyfél által adott adatkezelési hozzájárulást célonként külön - külön kell nyilvántartani (pl. kedvezményes utazási kártya kiállítása mellett az ügyfél hozzájárul részére marketing-üzenetek küldéséhez is), és biztosítani kell ezek egyenkénti visszavonásának lehetőségét.

A személyes adatokat a Társaság az adatkezelés céljához illeszkedő időtartamig (a panasz, észrevétel elintézéséig, az ügyfél által adott adatkezelési hozzájáruló nyilatkozat visszavonásáig, az érvényesített követelés statisztikai feldolgozásáig, stb.), illetve az ezekhez a műveletekhez kapcsolódó adóügyi, vagyoni védelmi és más előírások szerinti határidőig kezeli.

4.1.3. Az adatok minősége

A kezelt személyes adatoknak meg kell felelniük az alábbi követelményeknek:

- felvételük és kezelésük tisztességes és törvényes,
- pontosak, teljesek és időszerűek,
- tárolásuk módja alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani,
- nyilvántartásuk képes minden betekintés, beavatkozás, módosítás dokumentálására és így utólagos visszakeresésére.

4.1.4. Adatfeldolgozás

Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az Infotv., valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő – jelen esetben a Társaság – határozza meg. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel. Az adatfeldolgozó tevékenységi körén belül, illetőleg a Társaság által meghatározott keretek

között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért.

Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag a Társaság rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

Az adatfeldolgozásra vonatkozó megbízási szerződést – pl. személyes adatok adatbázisba rögzítése külső cég által, ügyfél-adatok nyilvántartása – írásba kell foglalni és a biztonsági vezető egyetértésével lehet megkötni. A szerződésben rögzíteni kell, hogy a Biztonság kijelölt munkavállalója ellenőrizni jogosult az adatfeldolgozás teljes folyamatát. Az adatfeldolgozásra nem adható megbízási olyan vállalkozásnak, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

4.1.5. Adattovábbítás, adatállományok összekapcsolása

Az adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.

Az előző bekezdést kell alkalmazni az ugyanazon adatkezelő, valamint az állami és az önkormányzati szervek által kezelt adatok összekapcsolására is.

Személyes adat az országból – az adathordozótól vagy az adatátvitel módjától függetlenül – más ország részére csak akkor továbbítható, ha az érintett ahhoz hozzájárult, vagy törvény azt lehetővé teszi, feltéve, hogy az adatkezelés Infotv. szerinti feltételei a külföldi ország részéről minden egyes adatra nézve teljesülnek.

4.1.6. Személyes adatok nyilvánosságra hozatala

Törvény közérdekből – az adatok körének kifejezett megjelölésével – elrendelheti a személyes adat nyilvánosságra hozatalát. Minden egyéb esetben a nyilvánosságra hozatalhoz az érintett hozzájárulása, különleges

adat esetében írásbeli hozzájárulása szükséges. Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

Ahol a szabályzat hozzájárulást, nyilatkozattételt, figyelemfelhívást, tájékoztatást említ, ott mindig írásos dokumentumot kell érteni az utólagos bizonyíthatóság érdekében.

Az érintett hozzájárulását megadottnak kell tekinteni az érintett közszereplése során általa közzölt, vagy a nyilvánosságra hozatal céljából általa átadott adatok tekintetében.

4.1.7. Az érintettek jogai

Az érintett

- tájékoztatást kérhet személyes adatai kezeléséről,
- kérheti személyes adatainak helyesbítését,
- kérheti a személyes adatainak törlését vagy zárolását a jogszabályban elrendelt adatkezelések kivételével.

Ha az ügyfél a Társaság valamelyik on-line rendszerében maga regisztrált, biztosítani kell részére a leregisztrálás jogát és lehetőségét is. Adatait az adatkezelés célja által meghatározott megőrzési idő figyelembe vételével kell a rendszerből törölni, más rendszerben, más célból kezelt és feldolgozott adatait azonban ez a törlés nem érintheti.

4.1.8. Jogorvoslati lehetőség

Az Infotv felhatalmazása alapján bárki a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (NAIH) kezdeményezhet vizsgálatot arra való hivatkozással, hogy személyes adatok kezelésével kapcsolatosan jogsérelem következett be, vagy annak közvetlen veszélye fennáll. A Társaság dolgozója emellett a biztonsági vezetőhöz vagy a belső adatvédelmi felelőshöz is fordulhat, ha véleménye szerint személyes adatainak kezelésével kapcsolatban jogsérelem érte, vagy annak közvetlen veszélye fennáll, kivéve, ha az adott ügyben bírósági eljárás van folyamatban.

A Hatósághoz, a biztonsági vezetőhöz és a belső adatvédelmi felelőshöz tett bejelentése miatt senkit sem érhet hátrány.

Az érintett a jogainak megsértése esetén, valamint az Infotv. 21. §-ában meghatározott esetekben az adatkezelő ellen bírósághoz fordulhat; ezen ügyekben a bíróság soron kívül jár el.

4.1.9. Adatbiztonság

Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek jelen utasítás, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelés megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek. A személyes adatokat tároló számítógépes adathordozóját teljes kapacitásában rejtjelezni szükséges pl.: TrueCrypt vagy vele azonos alkalmazással, operációs rendszer szolgáltatása által.

A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik. A szerver számítógépek és a munkaállomások között személyes adatok kizárólag védetten (rejtjelezve) továbbíthatók.

A Társaság alkalmazottainak személyes adatait tartalmazó – az IHIR-t kiegészítő, vagy más, pl. a távbeszélőhasználat forgalmi adatait kezelő – adatbázist létrehozni a belső adatvédelmi felelős előzetes egyetértésével, a biztonsági vezető engedélyével szabad. Ugyanezen szabályok vonatkoznak az ügyféladatokat kezelő rendszerekre is.

Az ilyen adatbázist az üzleti titok védelmére előírt szabályokkal azonos kategóriájú (a Társaság Informatikai Biztonsági Szabályzatában – IBSZ – definiált ún. „fokozott”) védelemben kell részesíteni. A rendszerekben a felhasználói jogosultságok korlátozásával biztosítani kell, hogy az egyes

ügyintézők 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 okmányok elkészültét követően szabad használatba venni és üzemeltetni.

Személyes adatot tartalmazó valamennyi dokumentum „Nem nyilvános!” kezelési jelzésű. A jelzést a dokumentum (pl. munkaszerződés, fizetési besorolás, az IHIR adatbázis felhasználásával készített Excel-táblázat, Utasleadási lap, kedvezményes utazásra jogosító kártya igénylőlapja) minden egyes lapjának fejrészében 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 illetéktelenül ne ismerhessék meg a mások képernyőn megjelenő személyes adatokat.

Személyes adat másolása az elektronikus adathordozók közül kizárólag CD-re és DVD-re megengedett, amin fel kell tüntetni a papír alapú adathordozóra előírt „Nem nyilvános” kezelési jelzést és az iktatószámot. Az így megjelölt dokumentumokat és adathordozókat biztonsági zárral ellátott fa iratszekrényben, vagy vas lemezszekrényben kell tárolni. A rontott és a munkapéldányokat megsemmisítésükig ugyanezen szabályok szerint kell tárolni; megsemmisítésük iratmegsemmisítővel / szétvagdosással történhet.

4.2. Az adatkezelésben közreműködők és feladataik

A Társaságnál folyó adatkezelések irányításában, ellenőrzésében és végzésében közreműködik:

- a) a Biztonság állományában:
 - biztonsági vezető,
 - a Társaság belső adatvédelmi felelőse,
 - információvédelmi szakértő,
 - területi biztonsági szakértő.

- b) a Társaság munkaszervezeteinél:
- munkáltatói jogkört gyakorló vezető,
 - közvetlen vezető,
 - a 4.3 Egyes adatkezelések c. fejezetben leírt üzleti, nyilvántartási, üzemi, technológiai, stb. folyamat végzése során személyes adatokat kezelő munkatársak,
 - belső ellenőrzési vezető és munkatársai,
 - Jog szervezet vezetője és munkatársai, a 4.2.9. pontban foglaltak szerint,
 - üzleti tulajdonos.

4.2.1. Biztonsági vezető

- a) a Társaság belső adatvédelmi felelőse útján irányítja és ellenőrzi az adatvédelemmel kapcsolatos előírások végrehajtását,
- b) felügyeli a Társaságnál keletkezett és más szervek által átadott személyes adatok védelmi rendszerének adminisztratív, személyi biztonsági, technikai, fizikai, kommunikációs, ellenőrzési és felügyeleti elemeken alapuló kiépítését és működését,
- c) az adatvédelemmel kapcsolatos feladatok végrehajtására egyedi ügyekben állásfoglalást, általános ügyekben útmutatót ad ki,
- d) szakmailag véleményezi az adatfeldolgozásra vonatkozó megbízási szerződést,
- e) évente értékeli a Társaság adatvédelmi helyzetét és arról írásban beszámol a Társaság vezérigazgatójának,
- f) az adatvédelmi feladatok ellátása során kapcsolatot tart a hatóságokkal.

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

4.2.2. A Társaság belső adatvédelmi felelőse

A biztonsági vezetőnek a felügyelete alá tartozó – jogi, közigazgatási, számítástechnikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező – belső adatvédelmi felelőst kell megbízni e szabályzatban foglalt feladat- és hatáskörrel az Infotv.-ből származó feladatok végzésére, irányítására, végrehajtásának ellenőrzésére, az adatkezelés feltételrendszerének kialakítására és fenntartására.

A funkciót a Biztonság információbiztonsági koordinátora gyakorolja. Feladatai:

- a) az információvédelmi szakértők közreműködésével ellátja a Társaság szervezeti egységei adatvédelmi tevékenységének szakirányítását és szakfelügyeletét,
- b) dönt a hatáskörébe tartozó, az adatkezeléssel összefüggő kérdésekben és előkészíti a döntéseket a hatáskörét meghaladó kérdésekben,
- c) ellenőrzi az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen utasítás rendelkezéseinek a betartását, figyelemmel kíséri az adatkezelésre vonatkozó jogszabályi változásokat,
- d) az Infotv. szerint bejelenti a Társaságnál végzett adatkezeléseket,
- e) az adatkezelő rendszerekben és számítógépes alkalmazásokban ellenőrzi az adatbiztonsági követelmények megvalósulását,
- f) kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén jelentést tesz a vezérigazgatónak a szolgálati út betartásával,
- g) elkészíti, évente felülvizsgálja és a szükséges gyakorisággal aktualizálja a Társaság Adatvédelmi Szabályzatát,
- h) állást foglal az adatkezeléssel kapcsolatos belső és külső megkeresésekben,
- i) szakmai segítséget nyújt az adatkezelők részére,
- j) rendszeresen ellenőrzi a személyes adatok kezelését,
- k) rendszeresen tájékoztatja a biztonsági vezetőt a folyó adatkezelésekről, a kezelőkről, a kezelt adatok köréről és a kezelés jogi megalapozottságáról,
- l) koordinál az egyes szervezeti egységek között az egységes adatvédelmi szemlélet megvalósítása érdekében,
- m) az előírásoknak nem megfelelő adatkezelés gyanúja esetén intézkedik annak kivizsgálására, kezdeményezi a szabálytalanságot eredményező tényezők megszüntetését,
- n) gondoskodik az adatvédelmi ismeretek oktatásáról,
- o) elvégzi az adatkezelések jogszabály által előírt bejelentését a NAIH részére,
- p) vezeti a belső adatvédelmi nyilvántartást, amelynek alapján kezdeményezi a NAIH felé az Infotv.-ben meghatározott engedélyezési eljárás lefolytatását,

q) támogatja az adatkezelőt vagy adatfeldolgozót a jogszabályi előírások teljesítésében.

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

4.2.3. Információvédelmi szakértő

- részt vesz az adatvédelmi normák kidolgozásában és karbantartásában,
- ellenőrzi a számítógépeken és az elektronikus adathordozókon a személyes adatok, ezek felhasználásával készült dokumentumok, előzmények, munkapéldányok kezelését, továbbítását, törlését, illetve az adathordozók előírásnak megfelelő tárolását,
- részt vesz az adatvédelem terén bekövetkezett, a hatályos szabályokat sértő események, veszélyeztetések kivizsgálásában,
- szakmai segítséget nyújt az adatkezelők részére,
- részt vesz az adatvédelmi oktatások előkészítésében és lebonyolításában.

A Társaságnál végzett adatvédelmi ellenőrzés során jogosult a szükséges mélységben betekinteni az ellenőrzés tárgyát képező adatkezelés és adatfeldolgozás anyagaiba, és jogosult teljes körű tájékoztatást kapni a vizsgált adatkezelésről.

4.2.4 Területi biztonsági szakértő

- szakmai segítséget nyújt az adatkezelők részére,
- részt vesz a területén bekövetkezett, az adatvédelemmel összefüggő incidensek kivizsgálásában,
- ellenőrzi a számítógépeken, elektronikus adathordozókon a személyes adatok, illetve ezek felhasználásával készült dokumentumok kezelését, a dokumentumok megfelelő tárolását,
- közreműködik a Társaság adatvédelmi és adatbiztonsági szabályzatának elkészítésében és aktualizálásában,
- támogatást ad az adatvédelmi oktatások előkészítéséhez, illetve lebonyolításához.

4.2.5. Munkáltatói jogkört gyakorló vezető

- szervezeti egységénél gondoskodik jelen szabályzat előírásainak végrehajtásáról,
- az irányítása alatt munkaviszonyban álló dolgozók szervezeténél nyilvántartott személyes adatainak védelmére intézkedik,
- a szabályostól eltérő adatkezelési gyakorlatot megszünteti, az ügy kivizsgálása érdekében értesíti a biztonsági vezetőt, vagy a belső adatvédelmi felelőst,
- irányítja és ellenőrzi a személyes adatok kezelésével, a személyes adatokat tartalmazó dokumentumok készítésével, továbbításával összefüggő adatvédelmi tevékenységét.

4.2.6. Közvetlen vezető

- felelős azért, hogy közvetlen beosztottja – akinek a Társaság számítógépet, e-mail címet biztosított – új munkakörbe kerülésekor, vagy a Társaság szervezetének elhagyásakor a munkakör átadás-átvétele során a számítógépén, a hálózati meghajtókon, valamint a levelező rendszerben levő postafiókjában tárolt magán jellegű és személyes adatait tartalmazó anyagait eltávolítsa, és a munkája során kezelt anyagokat, az ügyviteli és iktatási rendszerben kezelt iratokat, ügyiratokat átadja,
- a Társaság számára fontos és nélkülözhetetlen információk védelme érdekében az anyagok és információk átadásakor, a nem szükségesek törlésekor a közvetlen vezetőnek személyesen kell jelen lennie.

4.2.7. Személyes adatokat kezelő munkatárs

A Társaságnak az a munkavállalója, aki a 4.3 pontban felsorolt tevékenységek végzése során a személyes adatokon bármely műveletet végez, például gyűjt, felvesz, rögzít, rendszerez, tárol, megváltoztat, felhasznál, továbbít, nyilvánosságra hoz, összekapcsol, zárol, töröl, megsemmisít, annak további felhasználását megakadályozza, személyekről fénykép-, hang- vagy képfelvételt készít, vagy a személy azonosítására alkalmas fizikai jellemzőit (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzíti, köteles gondoskodni róla, hogy

- munkája során jelen szabályzat előírásai érvényesüljenek, biztosítva, hogy a személyes adatot tartalmazó dokumentum, adathordozó a keletkezésétől, illetőleg beérkezésétől kezdve előírás szerűen legyen kezelve és az ügyintézés befejezéséig tárolva,

- b) az általa készített vagy más szervtől érkezett, és neki ügyintézésre átadott személyes adatot tartalmazó dokumentumok és elektronikus adathordozók átvétele-átadása, nyilvántartásba vétele, rajtuk a „Nem nyilvános” minősítés és az iktatószám elhelyezése szabályosan történjen,
- c) a munka- és a rontott példányok előírás-szerűen meg legyenek megsemmisítve,
- d) a számítógépen keletkezett ideiglenes állományok biztonságosan, vissza nem állíthatóan kerüljenek törlésre,
- e) a személyes adatot tartalmazó dokumentum és elektronikus adathordozó az ügy elintézését követően a lehető legrövidebb időn belül visszakerüljön ahhoz, akitől munkavégzésre átvette,
- f) minden munkavállaló, akinek tudomására jut, hogy a Társaság, vagy annak adatfeldolgozója által kezelt személyes adat jogosulatlan személy tudomására jutott, vagy jogsértő módon került továbbításra, köteles erről a Társaság adatvédelmi felelősét tájékoztatni. Az adatvédelmi felelős intézkedik az eset körülményeinek feltárásáról és az adatkezelő szerv vezetőjén keresztül gondoskodik az érintett haladéktalan tájékoztatásáról.

4.2.8. *Belső ellenőrzési vezető és munkatársai*

A belső ellenőrzési vezető és az ellenőrzési szakértők az ellenőrzés céljához illeszkedő, az ellenőrzési tervben, Vizsgálati Programban, stb. előzetesen rögzített feladatkörben külön engedély nélkül megismerhetik a személyes adatot. A külön engedély nélküli hozzáférés az ellenőrzési terven kívüli, eseti célvizsgálatokra is vonatkozik.

4.2.9 *Jogi vezető*

Támogatja az adatkezelőt vagy adatfeldolgozót a jogszabályi előírások teljesítésében, a NAIH Társaságot érintő intézkedése esetén.

4.2.10 *Üzleti tulajdonos*

- a) az általa tulajdonolt rendszer vonatkozásában gondoskodik az adatvédelmi szabályok érvényre juttatásáról, a rendszerben található személyes adatok védelméről,
- b) intézkedik a nem szabályszerű adatkezelési gyakorlat megszüntetéséről, az eset kivizsgálása érdekében értesíti az adatvédelmi felelőst,

- c) az általa tulajdonolt rendszer tekintetében irányítja és ellenőrzi a személyes adatok kezelésével, azok készítésével, továbbításával összefüggő adatvédelmi tevékenységet.

4.3. *AZ EGYES ADATKEZELÉSEK*

A Társaságnál folytatott, az alábbi alcímek alatt felsorolt adatkezelések adatvédelmi megfelelőségét a következők szerint kell biztosítani.

4.3.1. *Személyazonosító adatok nyilvántartása*

A munkaviszony létesítésére szolgáló eljárás során a munkavállaló személyes adatainak forrása közvetlenül a munkavállaló. A munkaviszony létesítésére szolgáló eljárás keretében, a munkavállaló közreműködése nélkül, kizárólag a nyilvánosság számára, az érintett által korlátozás nélkül (pl. internet, sajtó) hozzáférhetővé tett információ használható fel, ideértve az érintett által kifejezetten a munkavállalásának elősegítése érdekében közzétett (pl. Twitter.com szakmai célú szociális háló útján rögzített) adatot. Harmadik személytől a munkavállaló a Mt. 81.§ (1) alapján, a Társaság azonban csak a munkavállaló előzetes hozzájárulásával kérheti a munkavállalóra vonatkozó személyes adat szolgáltatását.

A Munka Törvénykönyve rendelkezik a munkáltató által nyilvántartható adatok köréről, meghatározza, hogy a munkáltató a munkavállalótól csak olyan adatlap kitöltését kérheti, illetve vele szemben csak olyan alkalmassági vizsgálatot alkalmazhat, amely személyiségi jogait nem sérti, és a munkaviszony létesítése szempontjából lényeges tájékoztatást nyújthat. A törvény felhatalmazást ad a munkaidővel és a szabadságolással kapcsolatos adatok kezelésére is.

Ennek alapján a munkaszerződésben fel kell tüntetni azokat a természetes személyazonosító adatokat (név, anyja neve, születési hely és idő, lakcím), amelyek a munkavállaló egyértelmű azonosításához szükségesek. Más törvények a Társaság, mint munkáltató számára kötelezően előírják bizonyos személyes adatok kezelését. Így köteles nyilvántartani a munkavállaló adóazonosító jelét, társadalombiztosítási azonosító számát, mivel bevallási, illetve a különböző fizetési kötelezettségének csak azok alapján tud eleget tenni.

Olyan adat szolgáltatását a Társaság nem teheti kötelezővé, amely kezelésére törvényi felhatalmazása nincsen, így nem kezelheti például a munkavállalók személyi azonosítóját („személyi szám”).

A Társaság dolgozói személyi adatainak felvételét, az adatok számítógépes nyilvántartását a MÁV-csoport részére üzemeltetett IHIR elnevezésű rendszerben kell végezni. A rendszerben tárolt adatok meghatározása, az alkalmazás adatbázisának védelme az Infotv. rendelkezései alapján kialakított mindenkor hatályos MÁV-os és MÁV-START-os szabályzatok szerint történik.

A munkaviszony létesítésének bármely okból történő meghiúsulása esetén, a felvételi eljárás során rögzített személyes adatokat nyolc munkanapon belül törölni kell, kivéve, ha azok további kezeléséhez az érintett kifejezett hozzájárulását adta, illetve amennyiben arra jogszabályi előírás teljesítése érdekében van szükség.

A munkáltató részére megadott személyes adatok harmadik fél részére történő átadása kizárólag az érintett írásbeli hozzájárulásával történhet.

4.3.2. Munkabér nyilvántartása, kifizetése

Valamennyi dolgozó munkabérére és egyéb járandóságára vonatkozó információ különleges személyes adat, ezért megismertetése az érintetten kívüli személlyel tilos. A járandóságokat tartalmazó dokumentumot, tájékoztatót, listát, stb. az IHIR alkalmazás zárt rendszerben, illetéktelen megismerést kizáró munkafolyamatban, a szükséges védelmet szabályzatok által biztosítva állítja elő.

Ha a munkavállaló a járandóságát készpénzben veszi át (pl. kézipénztári kifizetések), akkor a kifizetés körülményeinek kell biztosítaniuk az adatok védelmét: egyszerre egy személy lehet a pénztárnál, a többi várakozó a biztonsági zónán kívül tartózkodjon, a munkavállaló pedig se a mások számára kifizetett pénzeszeget, se mások kifizetési listáját, elismervényét, stb. ne láthassa.

4.3.3 A munkavállaló tartózkodási helyének rögzítése

A munkavállaló tartózkodási helyének rögzítésére alkalmas technológiát (pl. GPS műholdas, vagy a GSM cellainformációs

helymeghatározás) a Társaság abban az esetben alkalmazhat, amennyiben az a munkavégzési célból a munkavállalók életének, testi épségének védelméhez, vagy munkájuk irányításához, illetve a vagyoni védelem erősítéséhez szükséges, feltéve, hogy az adatkezeléshez fűződő Társasági érdek a munkavállaló személyes adata védelméhez való jog korlátozásával arányban áll.

A munkavállalóról az általa vezetett gépjármű használata során történt GPS adatok felvétele a vele megkötött gépjármű használati megállapodásban rögzítettek szerint történhet. A Társaság a munkavállalóval megkötött gépjármű használati megállapodás részeként részletes tájékoztatást nyújt a munkavállaló számára a tartózkodási helyének rögzítésére alkalmas technológia alkalmazásáról és a rögzített adatok köréről, amely alapján minden használat megkezdésekor az önkéntes hozzájárulását megadja az adatainak kezeléséhez. A gépjármű magáncélú igénybevételre is feljogosított munkavállaló a magáncélú használat során keletkezett ilyen jellegű személyes adatát megfelelő törvényi jogalap, illetve a jogkorlátozással arányos adatkezelési cél hiányában a Társaság nem kezelheti, ezért biztosítani kell a magáncélú használat időtartama alatt, a helyadatgyűjtési szolgáltatás kikapcsolásának lehetőségét.

Biztosítani szükséges, hogy a gépjármű flottakezelője által megbízott helyadatgyűjtési szolgáltatás üzemeltetését végző gazdasági társaság ne juthasson munkavállaló azonosítását lehetővé tevő adatokhoz. A rögzített adatok a meghatározott céltól eltérő módon nem használhatók fel. Az adatokat az adatkezelés céljának megszűnésével, de legfeljebb egy év elteltével, illetve az érintett munkaviszonyának megszűnését/megszüntetését követően törölni kell.

A gépjármű használatával kapcsolatban felmerülő bármilyen jogvita esetén, annak jogerős lezárásáig, az adatok tovább kezelhetők.

4.3.4 Adattovábbítás EGT-n kívüli országba, illetve felhő alapú rendszerekbe

A Társaság munkavállalójának személyes adatát EGT-n kívüli országba csak az Infotv. által meghatározott feltételekkel, az érintett tevékeny, kizárólag erre a célra irányuló

hozzájárulása esetén továbbíthat, amennyiben az adatkezelés vagy adatfeldolgozás során megfelelő szinten biztosított a továbbított személyes adatok védelme. Ebbe a körbe tartoznak a „felhő alapú rendszerek”-ben kezelt személyes adatok is, amennyiben egyértelműen nem határozható meg az adatok tárolási helye.

4.3.5. Hatósági erkölcsi bizonyítványok kezelése

A hatósági erkölcsi bizonyítványhoz kötött munkakörökben dolgozó munkavállalók hatósági erkölcsi bizonyítvánnyal kötelesek igazolni, hogy nem szerepelnek Magyarország bűnügyi nyilvántartásában. A bizonyítványt a munkaszerződés megkötésével egyidejűleg a munkavállaló részére vissza kell szolgáltatni.

Amennyiben a munkavállaló a munkakör betöltésére a hatósági erkölcsi bizonyítvány alapján nem alkalmas, arról a visszaadást megelőzően másolatot kell készíteni, melyet kizárólag jogvita esetén lehet felhasználni, amelynek hiányában a másolatot egy év elteltével meg kell semmisíteni.

4.3.6. Összeférhetlenségi nyilatkozat kezelése

A mindenkor hatályos összeférhetlenség kezeléséről szóló belső utasítás alapján a Társasággal történő munkaszerződés megkötésekor, a foglalkoztatási viszonyaiban, vagy az összeférhetlenségi nyilatkozat tartalmában történt változásokat megelőzően tett összeférhetlenségi nyilatkozatot – a munkavállaló erre irányuló kérése esetén – zártan kell kezelni. A zárt kezelés lehetőségéről a munkavállalókat tájékoztatni kell. A vezető állású munkavállalóknak, vezető tisztségviselőknek, valamint a felügyelő bizottsági tagoknak mind saját személyükre, mind a közeli hozzátartozóikra vonatkozóan összeférhetlenségi nyilatkozatot, illetve bejelentést kell tenniük. Ebben az esetben szükséges az érintett hozzátartozó tájékoztatáson alapuló jognyilatkozatának beszerzése, amelyben hozzájárulnak személyes adataik Társaság által történő kezeléséhez, emellett a hozzátartozó számára is biztosítani kell a 4.1.7. pontban felsorolt jogokat. A munkáltatói jogkör gyakorlója az elbírált és záradékolt nyilatkozatokat a humánpartner útján küldi meg a Humán szervezet számára, az érintett szolgálati anyagában elhelyezés érdekében.

4.3.7. A videokamerás megfigyelések

A kamerarendszerek rendelkezésre állását az üzemeltetővel kötött szerződéssel, a velük végzett megfigyelések adatvédelmi megfelelőségét pedig a megfigyelést végzővel kötött, adatvédelmi szabályokat is tartalmazó szerződést írásba kell foglalni. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységében érdekelt. A vonatkamerás megfigyelések és az azzal végzett adatkezelés, adatfeldolgozás szabályait külön vezérgazgatói utasításban kell szabályozni.

4.3.7.1. A megfigyelés célja

A vasútállomáson a közforgalom számára nyitva álló helyen, a megállóhelyen valamint a személyszállító vasúti járművek belterében elhelyezett elektronikus megfigyelőrendszer működtetésének célja a vasútállomáson és megállóhelyen található berendezések, a személyszállító vasúti járművek, továbbá az utasok életének, személyének, testi épségének és vagyontárgyaik védelme, illetve a felsorolt körbe tartozó események utólagos vizsgálatának segítése.

Az üzemi és munkaterületeken, irodaházakban elhelyezett elektronikus megfigyelőrendszer működtetésének célja a vagyonvédelem: berendezések eltulajdonításának, megrongálásának megakadályozása, illetve a felsorolt körbe tartozó események utólagos vizsgálatának segítése.

4.3.7.2. Tájékoztatás a megfigyelésről

A kamerákat jól látható helyre kell felszerelni. Figyelmeztető, ismertető táblát kell elhelyezni – a vakok és gyengénlátók számára is érzékelhető módon – a vasútállomás és megállóhely bejáratánál, továbbá a személyszállító vasúti járműre való felszállásra szolgáló peronoknál, valamint a személyszállító vasúti járművön, amely tájékoztatást tartalmaz az elektronikus biztonságtechnikai rendszer által folytatott megfigyelés, valamint a rendszer által rögzített személyes adatokat tartalmazó kép- és hangfelvétel készítésének, tárolásának:

- céljáról,
- az adatkezelés jogalapjáról,
- a felvétel tárolásának helyéről,
- a tárolás időtartamáról,
- a rendszert alkalmazó (üzemeltető) személyéről,

- az adatok megismerésére jogosult személyek köréről, továbbá
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az érintett jogaira és érvényesítésük rendjére vonatkozó rendelkezéseiről

az alábbi, jól olvashatóan kiírt szöveggel:

a) ha a felvételeket elektronikusan rögzítik (jellemzően utasok, ügyfelek számára megnyitott területeken, egyes személyszállító járműveken, üzemi területeken, munkaterületeken, személypénztáraknál): 5. sz. melléklet

b) ahol a felvételeket nem rögzítik (jellemzően a Társaság irodaházaiban):

”Kamerával megfigyelt terület.

A megfigyelés célja vagyonvédelem. A felvételek nem kerülnek rögzítésre.”

4.3.7.3. A megfigyelési adatok megismerése

A megfigyelőrendszer által rögzített adatokhoz

- a) a biztonsági vezető által kijelölt személy,
- b) a bírósági vagy más hatósági eljárásban történő felhasználás érdekében a bíróság, illetve az eljárásra illetékes más hatóság férhet hozzá.

Az a) esetben a megismerésről a megismerésre jogosult személy – és lehetőség szerint az érintettek – nevének, az adatok megismerése okának és idejének rögzítésével jegyzőkönyvet kell felvenni, és azt a belső adatvédelmi felelősnél kell tárolni.

Az adatot olyan zárt rendszerben, illetve olyan eljárással kell kimenteni, amelyben biztosított, hogy azt a kimentésében közreműködők nem ismerhetik meg. A mentett adatot tartalmazó adathordozót a „Nem nyilvános” kezelési jelzés szerint kell megőrizni és továbbítani a belső adatvédelmi felelőshöz. A bíróság vagy más hatóság megkeresésére a kimentett képfelvételt a megkereső szerv részére – műszaki ellenőrzést követően – a biztonsági vezető küldi meg vagy adja át.

4.3.7.4. A megfigyelési adatok törlése

- a) Nem alkalmazható elektronikus megfigyelőrendszer olyan helyen, ahol a megfigyelés az emberi méltóságot sértheti, így különösen mosdóban, illemhelyen.

b) A rögzített kép, vagy kép- és hangfelvételt felhasználás hiányában a rögzítéstől számított 16. napon meg kell semmisíteni vagy törölni kell. Felhasználásnak minősül, ha a rögzített kép-, illetve hangfelvétel bírósági vagy hatósági eljárásban bizonyítékként felhasználásra vagy bíróság, hatóság részére ilyen eljárás során benyújtásra kerül.

c) Akinek jogát vagy jogos érdekét a b) bekezdés szerinti kép-, illetve hangfelvétel érinti, a rögzítéstől számított 15 napon belül jogának vagy jogos érdekének igazolásával kérheti, hogy a kép- illetve hangfelvételt annak kezelője ne semmisítse meg vagy ne törölje.

d) Bíróság vagy más hatóság megkeresésére a rögzített kép-, illetve hangfelvételt a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Ha a megkeresésre attól számított 72 órán belül, hogy a megsemmisítés vagy törlés mellőzését a c) bekezdés alapján kérték, nem kerül sor, és a b) bekezdésben meghatározott határidő letelt, a rögzített kép- illetve hangfelvételt meg kell semmisíteni, vagy törölni kell.

Amennyiben a kép-, hang-, vagy kép és hangfelvétel megőrzésének idején belül a rögzítéssel érintett személy jogának vagy jogos érdekének igazolásával kéri az adat megsemmisítésének elhalasztását, a megjelölt adatot ki kell menteni és át kell adni a belső adatvédelmi felelősnek. Az adat kiszolgáltatására irányuló bírósági, más hatósági megkeresésig, de legkésőbb az érintett személy kérelmének beérkezésétől számított 15 napig változatlan tartalommal a kimentett adatokat meg kell őrizni.

4.3.7.5. A munkahelyi számítógép, az e-mail és az Internet használatának ellenőrzése

A Társaság a munkavállalóknak indokolt esetben, munkavégzés céljára biztosít számítógépet, kommunikációs eszközöket, e-mail címet és Internet-hozzáférést. A használat szabályairól és a magáncélú használat ellenőrzésének lehetőségéről a munkavállalókat írásban kell tájékoztatni (1. számú melléklet). A tájékoztatásról és a munkavállaló hozzájárulásáról a munkavállaló által aláírt nyilatkozatot a Humán szervezetenél a dolgozó szolgálati táblájában meg kell őrizni.

A kizárólag munkavégzés céljából biztosított e-mail postafiók esetén a munkáltatónak joga van a postaládában lévő e-mailek fejlécének megtekintése után – ahol szerepel a küldő és a fogadó személye, e-mail címe, a levél megnevezése, a küldés időpontja, a levél mérete – konkrét levél kiadását kérni a munkavállalótól. A munkavállaló a levél átadását csak a harmadik személy jogát sértő levéltitokra történő hivatkozással tagadhatja meg. Abban az esetben, ha az e-mail postafiókot kizárólag hivatalos használatra adták át számára és a kért levelet a munkavállaló írta, vele szemben ez esetben is munkajogi szankciókat alkalmazhat a munkáltatói jogkörgyakorló.

Amennyiben egy munkavállaló tartós távolléte alatt, vagy munkaviszonyának megszűnését követően az email postafiókjának ellenőrzése szükséges, vagy indokolt, az érintett munkavállaló által a levelező rendszerben a postafiókjához hozzáféréssel rendelkező másik munkavállaló – ha ilyen személy nincs, vagy nem tartózkodik a munkahelyen, akkor a rendszer üzemeltetéséért felelős informatikus – jegyzőkönyv felvétele mellett betekinthez az e-mail postafiókba. Amelyik levélről egyértelműen megállapítható, hogy hivatalos tárgyú, átadható a munkáltatónak. Az érintett információs önrendelkezési jogának maradéktalan érvényesülése érdekében a távollévő érintettet tájékoztatni kell arról, hogy távollétében más személy az e-mail postafiók tartalmát megismerte.

A munkavállaló által használt e-mail postafiók ellenőrizhetősége érdekében az ellenőrzés pontos részleteiről, az ellenőrzést megelőzően megfelelő formában és módon tájékoztatást kell adni a munkavállaló számára. A tájékoztatásnak ki kell terjednie arra, hogy az adatkezelés milyen célból történik, ki az adatkezelő, mennyi ideig kezelik a felvett adatokat, illetőleg az adatkezeléssel kapcsolatban milyen jogai vannak az érintett személyeknek. A társaság által biztosított elektronikus levelező rendszer használata során, a személyes adatok védelme érdekében, az alábbi szabályokat kell betartani:

a) a levelező rendszer használata kizárólag hivatalos célra engedélyezett,
b) a több mint 50 e-mail címzett esetén a küldemény valamennyi címzettjét rejtett módon (titkos másolat mezőben) kell megadni a spam küldemények csökkentése érdekében,

c) amennyiben a címzettek között a MÁV levelezőrendszerén kívüli címzett is szerepel, vizsgálni kell a b) pontban leírt módszer alkalmazásának szükségességét,

d) QR kódot tartalmazó e-mailek küldése esetén fennáll annak a veszélye, hogy a továbbítás során illetéktelenek lecserélhetik azt, és a QR kódot előállító felhasználó tudta nélkül károkozásra használják fel, amely hátrányosan befolyásolhatja a Társaság megítélését. Ezért a QR kódoknak az e-mailek MÁV munkavállalója által elhelyezett aláírásában történő felhasználása a Társaság hivatalos elektronikus levelezésben nem megengedett,

e) a nagyobb mennyiségű személyes adatot tartalmazó küldemény továbbítása kizárólag technikai védelemmel (illetéktelen megnyitás ellen jelszóval védett Office dokumentumban, RMS védelemmel, jelszóval védett tömörített állományban stb.) engedélyezett. A személyes adatot tartalmazó elektronikus levelet a következő záradékkal kell ellátni:

„A jelen levélben kézbesített információ kizárólag a címzettnek szól, és bizalmas üzleti, illetve személyes adatokat tartalmazhat. Amennyiben nem Ön a levél címzettje, a levélben található információ felhasználása, vagy bármilyen módon történő közzététele, másolása vagy megosztása tilos. Amennyiben jelen levelet tévedésből kapta meg, kérem lépjen kapcsolatba a levél feladóival és az üzenetet haladéktalanul törölje a számítógépéről. A levél feladóinak e-mail címe kifejezetten vállalati felhasználásra szolgál, a biztonsági szervezet – vezetői ellenőrzés céljából – betekinthez tartalmába, kérem erre a címre magánjellegű küldeményt, reklámanyagot ne küldjön!”

A munkavállaló által használt e-mail postafiók ellenőrzését a munkáltatói jogkört gyakorló vezető egyidejű tájékoztatása mellett a Biztonság kijelölt szakértője végzi. Az ellenőrzés során biztosítani kell az ellenőrzött jelenlétét és magánszférájának sértetlenségét. A megismerésről a megismerésre jogosult személyek és az érintettek nevének, az adatok megismerése okának és idejének rögzítésével jegyzőkönyvet kell felvenni, és azt a belső adatvédelmi felelősnél kell tárolni.

A Társaság azon munkavállalója, akinek számítógépet, kommunikációs eszközt, e-mail címet és Internet-hozzáférést biztosított a Társaság, az eszköz leadásakor és átadásakor (különösen a Társaság szervezetének elhagyásakor és új munkakörbe kerülésekor) a munkakör átadás-átvétele során köteles a számítógépen, a hálózati meghajtókon és a levelező rendszerben lévő postafiókjában – a tiltás ellenére esetleg – tárolt magán jellegű, és személyes adatait tartalmazó anyagait (dokumentumok, táblázatok, bemutatók, programok, levelek, zenék, fényképek, videók, stb.) eltávolítani. A folyamat ellenőrzéséért a dolgozó közvetlen vezetője felelős. A folyamat végrehajtását dokumentálni kell (2. számú melléklet). A munkavállaló által aláírt nyilatkozatot a Humán szervezetnél a dolgozó szolgálati táblájában meg kell őrizni.

A munkaviszonnal összefüggő, infokommunikációs eszközökön elektronikus formában tárolt állományokat, dokumentumokat, elektronikus levelezést a munkakör átadásakor a munkavállaló köteles a munkáltatói jogkört gyakorló vezető ellenőrzése mellett, az informatikai üzemeltető szakértőjének közreműködésével az utódjának, ennek hiányában a munkáltatói jogkört gyakorló vezetőnek dokumentált módon átadni.

4.3.7.6. A távolról végzett munka

Amennyiben a munkafeladatok ellátása távolról végzett munka útján valósul meg (pl. VPN kapcsolaton keresztül), és az nem a Társaság által biztosított eszköz igénybevételével történik, a Társaság nem tekinthet be az eszközön tárolt, nem a munkaviszonnal összefüggő adatokba. Amennyiben a távmunkához a Társaság kizárólag munkavégzés céljára biztosítja az eszközt, a tilalom betartásának ellenőrzése céljából a Társaság – a 4.3.7.6. pontban foglaltak értelemszerű alkalmazásával – a teljes adattartalmat ellenőrizheti.

4.3.7.7. Forgalomtechnológiai okokból végzett hangrögzítés

Ide tartozik a diszpécsertelefon, a mozdonyrádió és bármely forgalomtechnológiai szolgálati célra használt, MÁV-START Zrt. tulajdonú vagy üzemeltetésű hangkommunikációs eszköz. Ezen eszközökön magáncélú beszélgetés tilos. A Társaság a teljes

beszédforgalmat rögzítheti és ellenőrizheti. A használat szabályairól és a magáncélú használat ellenőrzésének lehetőségéről az érintett munkakörben dolgozó munkavállalókat írásban kell tájékoztatni (3. számú melléklet). A tájékoztatásról és a munkavállaló hozzájárulásáról a munkavállaló által aláírt nyilatkozatot a Humán szervezetnél a dolgozó szolgálati táblájában meg kell őrizni.

A Társaság területén forgalomtechnológiai okokból végzett hangrögzítés során a hangrögzítő berendezéseken rögzített adatokat a munkáltatói jogokat gyakorló vezető, a Biztonság vasútbiztonsági területének munkatársa, baleset esetén a balesetvizsgáló csoport vezetője hallgathatja vissza. A keletkezett adatokat a fenti személyek írásban rögzíthetik, illetve további vizsgálat céljából azokat lemásolhatják és maguknál tarthatják, valamint a vizsgálat során bizonyítékként felhasználhatják.

A megismerésről a megismerésre jogosult személyek és az érintettek nevének, az adatok megismerése okának és idejének rögzítésével jegyzőkönyvet kell felvenni, és azt a belső adatvédelmi felelősnél kell tárolni.

4.3.7.8. Távbeszélő-használat forgalmi adatainak kezelése

A távbeszélőforgalmat nyilvántartó rendszer a személyes adatok körébe tartozó telefonhívási adatokat kezel és listákat állít elő, azok alapján számlázási alapadatokat szolgáltat. A listák készítője köteles azokra a „Nem nyilvános” kezelési jelzést és iktatási számot felvezetni, és a dokumentumokat a továbbiakban eszerint kezelni.

A távbeszélőforgalmat nyilvántartó számítógépes rendszert a 4.1.9. Adatbiztonság c. fejezetben foglalt szabályok betartásával szabad létrehozni és üzemeltetni.

A nyilvántartó rendszer kialakítása során figyelembe kell venni, hogy a dolgozó az Adatvédelmi nyilatkozat aláírásával hozzájárulását adja egyes személyes adatainak a munkáltató általi kezeléséhez, azonban a dolgozóval telefonbeszélgetést folytató külső fél nem tesz ilyen nyilatkozatot, ezért a személyes adatát képező teljes hívószámát a rendszer nem rögzítheti, csupán annak részeit.

Abban az esetben, ha a munkavállaló túllépte a részére irányadó beszéd- vagy adatforgalmazási költségkeretet, és vele szemben költségtérítési eljárás indul, az eljárásban a hívott fél hívószáma nem használható fel, csak a hívásköltség lista anonimizált, vagyis hívószám feltüntetése nélküli módon.

4.3.7.9. Ügyfeladatok kezelése

Épületekbe való belépést dokumentáló nyilvántartások, Utasok könyvének vezetése, panaszos levelek, Utasleadási lapok, kedvezményes utazásra jogosító igazolványok és kártyák stb. ügyintézése során a Társaság birtokába, illetve kezelésébe nagy számban kerülnek a Társasággal munkaviszonyban nem álló személyek személyes adatai. Ezen adatokat a Társaság munkaszervezetei az Infotv. értelmében a saját dolgozók személyes adataival megegyező szintű védelem biztosítása mellett kötelesek kezelni.

Az adatfelvételi nyomtatványokon, elektronikus űrlapokon az érintett írásos hozzájárulását kell kérni adatainak kezeléséhez. Ha az utassal szembeni követelés behajtásával, vagy a kedvezményes kártyák elkészítésével, stb. a Társaság várhatóan harmadik felet bíz meg, akkor előzetesen ki kell kérni (célszerűen már az adatfelvételi lapon) az érintett beleegyezését adatai ún. harmadik személy (az adatfeldolgozó) részére történő átadásához.

Az adatfelvételi lapon rövid adatvédelmi tájékoztatást kell elhelyezni a Társaságnál folyó adatkezelés elveiről. Az internet útján elérhető (on-line) elektronikus adatfelvételi lapokon a Társaság honlapján található Adatvédelmi tájékoztatóra mutató linket kell elhelyezni.

Ha az ügyfél élőszóban keresi meg a Társaság ügyfélszolgálatát, akkor az adatvédelmi tájékoztatást élőszóban vagy gépi hangbemondással kell részére megadni. Egyúttal beleegyezését kell kérni a kommunikáció rögzítéséhez. Engedélyének hiányában személyes ügyfélkapcsolathoz kell irányítani. A tájékoztató szövegét előzőleg egyeztetni kell a Társaság belső adatvédelmi felelősével.

Az adatfelvételhez használt elektronikus input bizonylatokra és papír alapú lapokra, nyomtatványokra (pl. Utasleadási lap, Utasok könyve) rá kell vezetni a „Kitöltés után nem nyilvános” kezelési jelzést, és a továbbiakban a

tárolást, megőrzést, megsemmisítést ennek megfelelően kell végezni.

Az ügyfeladatokat rögzítő, kezelő és feldolgozó szervezeti egységeknek gondoskodniuk kell, arról, hogy a személyes adatokat tartalmazó dokumentumokat, nyomtatványokban, könyvekben stb. maradt lapokat, tözselvényeket (pl. Utasleadási Lap, Utasok könyve) illetéktelen személy ne ismerhesse meg, és azok a kezelési jelzésnek megfelelően kerüljenek tárolásra.

Az ügyfeladatokat feldolgozó számítógépes rendszert a 4.1.9. Adatbiztonság c. fejezetben írtak betartásával szabad létrehozni és üzemeltetni.

A Társaság az ügyfelek adatainak nyilvántartásáról a honlapján közzéteszi az Adatvédelmi tájékoztatót (4. számú melléklet).

4.3.7.10. A Társaság telefonos ügyfélszolgálat, MÁVDIREKT telefonbeszélgetéseinek kezelése

Az Utas kérelmezheti az adatkezelőtől személyes adatai (hangfelvétel) másolatának megküldését az Infotv. 14-18. § előírásainak figyelembevételével.

4.3.7.11. Adatfelvétel és kezelés mozgáskorlátozottak utazásához

Összhangban a Személyszállítási Üzletszabályzat II. fejezet 9. cím 9.5. pontjával, a mozgáskorlátozott, kerekesszékekkel együtt utazók szállításának minél zökkenőmentesebb lebonyolítása érdekében a Társaság lehetőséget kíván biztosítani a rendszeresen vasúton utazó mozgáskorlátozottak személyazonosító adatai rögzítésére.

Az Ügyfélszolgálati Központnál a kerekesszékekkel történő utazás bejelentése egy erre rendszeresített – honlapról is letölthető – egyedi formanyomtatványon történik. Az adatlap statikus (pl. név, cím, elérhetőség, kerekesszék adatai) és dinamikus (utazás paraméterei) adatokat egyaránt tartalmaz. Az igénybejelentőnek a kezdeti adatfeltöltést követően a további utazások alkalmával (adategyeztetést követően) csupán az utazás időpontjára vonatkozó adatokat szükséges megadnia a bejelentésében.

4.3.7.12 Az értekezleteken készülő hangfelvétel
Az értekezleteken készülő hangfelvétel valamennyi érintett hozzájárulásával kezelhető. Az elhangzottak rögzítése kizárólag az érintettek tájékoztatását követő kifejezett hozzájárulása után történhet. A tájékoztatás megtörténtének és a hozzájárulások megadásának dokumentálása történhet a résztvevők jelenlétében a hangrögzítő eszközre történő bemonddással, vagy a jelenléti ív aláírásával, az azon szereplő írásos tájékoztató egyidejű elfogadásával. A felvétel célja elsősorban a megbeszélésekről készített jegyzőkönyv, emlékeztető pontos elkészítése, a megbeszélésen elhangzottak szöveghű visszaidézése. Ennek érdekében a hangfelvételt, a felhasználásával készített írott dokumentum jóváhagyását követően, visszaállíthatatlan módon törölni szükséges. Különösen indokolt esetben – valamennyi érintett kifejezett hozzájárulása esetén – a felvétel csatolható az elkészített emlékeztetőhöz.

4.3.7.13. Videokonferencia

Videokonferencia szervezése esetén készülő felvétel valamennyi érintett hozzájárulásával kezelhető. Az elhangzottak rögzítése kizárólag az érintettek tájékoztatása és hozzájárulása után történhet. A tájékoztatás megtörténtének és a hozzájárulások megadásának dokumentálása történhet a résztvevők jelenlétében a felvételre történő bemonddással, illetve a jelenléti ív aláírásával, az azon szereplő írásos tájékoztató egyidejű elfogadásával. A videokonferencia felvételének elsődleges célja a megbeszélés kép- és hang anyagának dokumentálása, az arról készített jegyzőkönyv, emlékeztető pontos elkészítése, a megbeszélésen elhangzottak kép- és szöveghű visszaidézése. Ennek érdekében a felvételt, a felhasználásával készített írott dokumentum jóváhagyását követően, visszaállíthatatlan módon törölni szükséges. Különösen indokolt esetben – valamennyi érintett kifejezett hozzájárulása esetén – a felvétel csatolható az elkészített emlékeztetőhöz.

4.4 Egyéb rendelkezések

Az adatvédelmi ismereteket jelen szabályzat alapján a Társasághoz való belépéskor minden munkavállaló számára oktatni kell. Az oktatásért és a nyilatkozat levételéért a Humán felvételt végző munkatársa felelős.

A munkáltatói jogkört gyakorló vezetőket, továbbá az egyes adatkezelések c. fejezetben írt adatkezeléseket végzőket évente egy óras utóképzésben kell részesíteni. Az oktatás és az éves képzés végrehajtásáért a Biztonság vezetője felelős.

5.0 HIVATKOZÁSOK, BIZONYLATOK MÓDOSÍTÁSOK HATÁLYON KÍVÜL HELYEZÉSEK

5.1. Hivatkozások

- 2012. évi I. törvény a Munka Törvénykönyvéről
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
- 2012. évi XLI. törvény a személyszállítási szolgáltatásokról
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 1/2007. (I.5. MÁV Ért. 1.) HVH sz. humánpol. vezig-h. ut. a személyügyi adatok kezeléséről a MÁV Zrt.-ben
- a MÁV-START Zrt. mindenkor hatályos Vagyonvédelmi szabályzata
- a MÁV-START Zrt. mindenkor hatályos Üzletititok-védelmi Szabályzata
- a MÁV-START Zrt. mindenkor hatályos Informatikai Biztonsági Szabályzata
- A MÁV-START Zrt. mindenkor hatályos vezérigazgatói utasítása a személyszállító vonatok biztonsági kamerarendszerével rögzített felvételek kezeléséről
- a MÁV-START Zrt. mindenkor hatályos Közvetélteli Szabályzata

5.2. Hatályon kívül helyezés

Az utasítás hatályba lépésével egyidejűleg hatályát veszti a 8/2010. (IV.2. MÁV-START Ért. 4.) VIG sz. vezérigazgatói utasítás a MÁV-START Zrt. Adatvédelmi Szabályzatáról szóló 19/2008. (IV.11. MÁV-START Ért. 6) VIG sz. vezérigazgatói utasítás 1. sz. módosításáról (egységes szerkezetben).

6.0. HATÁLYBA LÉPTETÉS

Jelen szabályzat előírásait a MÁV-TRAKCIÓ Zrt.-nek és a MÁV-GÉPÉSZET Zrt.-nek a MÁV-START Zrt.-be történő beolvadása napjától kezdődő hatállyal kell alkalmazni.

7.0. MELLÉKLETEK

1. sz.: Adatvédelmi tájékoztató és nyilatkozat
2. sz.: Nyilatkozat magánjellegű és személyes adatok eltávolításáról
3. sz.: Adatvédelmi tájékoztató és nyilatkozat
4. sz.: Társaság adatvédelmi tájékoztatója
5. sz. Adatvédelmi tájékoztató matrica

Ungvári Csaba s.k.
vezérigazgató

ADATVÉDELMI TÁJÉKOZTATÓ ÉS NYILATKOZAT 1**INFORMATIKAI ÉS INFOKOMMUNIKÁCIÓS ESZKÖZÖK HASZNÁLATÁRÓL**

A MÁV-START Zrt. indokolt esetben a munkakörhöz kapcsolódó feladatok elvégzése céljából munkahelyi számítógépet, okostelefont, egyéb informatikai és infokommunikációs eszközt, elektronikus levelezési címet, belső hálózati tárhely hozzáférést és Internet-hozzáférést biztosít a munkavállalóknak. A fenti eszközök munkavégzés céljára szolgálnak, a velük végzett tevékenységet a MÁV-START Zrt. esetenként ellenőrzi. Nem előírászerű használat esetén a használati jog megvonásra kerülhet, a biztonság szándékos megkerülése tényfeltáró vizsgálatot, illetve hátrányos jogkövetkezmény megállapítására vonatkozó munkáltatói intézkedést vonhat maga után.

Jogainak megsértése esetén az érintett munkavállaló az adatkezelő ellen bírósághoz fordulhat, illetve kezdeményezheti a Nemzeti Adatvédelmi és Információszabadság Hatóság eljárását.

NYILATKOZAT

Alulírott (anyja neve:.....,
szül. hely:....., szül. idő:.....) a fenti tájékoztatást tudomásul
vettem. Beleegyezem, hogy a MÁV-START Zrt. a fenti eszközök általam történő használatát
ellenőrizze.

dátum:
munkavállaló aláírása

A nyilatkozatot a MÁV-START Zrt. megbízásából átvettem:

.....

név aláírás

Készült 2 pld-ban.

1. sz. pld.: érintett

2. sz. pld.: MÁV-START Zrt. Humán

NYILATKOZAT
magánjellegű és személyes adatok eltávolításáról

Alulírott (anya neve:.....,
szül. hely:....., szül. idő:.....) elismerem, hogy a
MÁV-START Zrt. munkavégzés céljából részemre:

- munkahelyi számítógépet,
- hordozható számítógépet,
- informatikai hálózati hozzáférést,
- kézi számítógépet (PDA, Palm PC),
- elektronikus levelezési címet
- Internet-hozzáférést
- Okostelefon
-

biztosított.

Kijelentem, hogy a mai napon a fent felsorolt eszközökön, a hálózati meghajtókon és a levelező rendszerben lévő postafiókomban az általam használt anyagokat (dokumentumok, táblázatok, bemutatók, programok, levelek, zenék, fényképek, videók) leellenőriztem. A magánjellegű és személyes adataimat tartalmazó anyagokat eltávolítottam.

dátum:

.....

munkavállaló aláírása

A nyilatkozatot a MÁV-START Zrt. megbízásából átvettem:

.....

név

.....

aláírás

Készült 2 pld-ban.

1. sz. pld.: érintett

2. sz. pld.: MÁV-START Zrt. Humán

ADATVÉDELMI TÁJÉKOZTATÓ ÉS NYILATKOZAT 2
KOMMUNIKÁCIÓS ESZKÖZÖK HASZNÁLATÁRÓL

A MÁV-START Zrt. indokolt esetben diszpécsertelefont, mozdonyrádiót, vagy más kommunikációs eszközt biztosít a munkavállalóknak. A fenti eszközök munkavégzés céljára szolgálnak, a velük végzett tevékenységet a MÁV-START Zrt. esetenként ellenőrzi. Nem előírászerű használat esetén a használati jog megvonásra kerülhet.

NYILATKOZAT

Alulírott (anya neve:.....,
szül. hely:....., szül. idő:.....) a fenti tájékoztatást tudomásul
vettem. Beleegyezem, hogy a MÁV-START Zrt. a fenti eszközök általam történő használatát
ellenőrizze.

dátum:

.....
munkavállaló aláírása

A nyilatkozatot a MÁV-START Zrt. megbízásából átvettem:

.....
név.....
aláírás

Készült 2 pld-ban.

1. sz. pld.: érintett

2. sz. pld.: MÁV-START Zrt. Humán

ADATVÉDELMI TÁJÉKOZTATÓ

A MÁV-START Vasúti Személyszállító Zrt. (továbbiakban: MÁV-START Zrt.) az utasainak és más ügyfeleinek a személyes adatát az alábbi célok érdekében kezeli:

- részükre menetjegyek és helyjegyek biztosítása és azok nyilvántartása,
- kedvezményes utazásra jogosító kártyák és igazolványok elkészítése, nyilvántartása, használatának ellenőrzése,
- panaszok és észrevételek intézése,
- utazás alatti vagyonvédelem és testi épség biztosítása,
- a velük szemben fennálló követelések érvényesítése.

Az ilyen adatkezeléshez az utas a menet- és helyjegy-igényének kinyilvánítása, illetve a kártya, az igazolvány igénylése, továbbá az észrevételének vagy panaszának közlése során tett nyilatkozatával; illetve (tájékozott beleegyezést követően) az utazás megkezdésével járul hozzá. A felsoroltaktól eltérő (pl. marketing) célok esetében a MÁV-START Zrt. kizárólag akkor kezeli utasa és más ügyfele személyes adatát, ha az adatkezelés céljáról az érintettet tájékoztatta, és ahhoz az érintett kifejezetten hozzájárult.

A személyes adatokat az adatkezelés céljához illeszkedő időtartamig (a panasz, észrevétel elintézéséig, a hozzájáruló nyilatkozat visszavonásáig, az érvényesített követelés statisztikai feldolgozásáig, stb.), illetve az ezekhez a műveletekhez kapcsolódó adóügyi, vagyonvédelmi és más előírások szerinti határidőig kezeli.

A MÁV-START Zrt. kötelezi magát arra, hogy gondoskodik utasai és más ügyfelei általa kezelt személyes adatainak biztonságáról. Megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat a belső eljárási szabályokat, amelyek biztosítják, hogy a kezelt (felvett, tárolt, stb.) adatok védettek legyenek. A személyes adatokat fokozott biztonságú informatikai rendszerekben, nem nyilvános módon kezeli. Megakadályozza azok véletlen megsemmisülését, jogosulatlan felhasználását és jogosulatlan megváltoztatását. Biztosítja, hogy a személyes adatokat csak az illetékes munkakörök betöltő személyek ismerhessék meg, magas szintű hozzáférési kontrollok alkalmazása mellett. Az internet használatával továbbításra kerülő adatok tekintetében fokozott biztonságú védelmi intézkedéseket tesz.

A MÁV-START Zrt. a rendelkezésére bocsátott személyes adatok feldolgozásához – az érintett hozzájárulásával – külső adatfeldolgozót vehet igénybe, amely a neki átadott adatokon csak technikai műveleteket végez (például számítógépes rendszerben való tárolás, megőrzés). A MÁV-START Zrt. a külső félnél végzett adatfeldolgozás jogszerűségéért ugyanúgy felel, mint saját adatkezeléséért, amit az adatfeldolgozóval kötött írásos szerződéssel biztosít. A MÁV-START Zrt. kötelezi magát arra is, hogy adatvédelmi kötelezettségeinek teljesítésére felhívja minden olyan harmadik fél figyelmét, amelynek az adatokat továbbítja vagy átadja.

Az utas a MÁV-START Zrt. Központi Ügyfélszolgálatán (levélben: 1426 Budapest, Pf.: 56., telefonon: MÁVDIREKT 06 (40) 49 49 49, külföldről hívható +36 (1) 444 44 99, faxon: +36-1-511-2093, e-mailben: eszrevetel@mav-start.hu) bármikor tájékoztatást kérhet kezelt személyes adatairól, kérheti azok helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – az adatbázisból való törlését.

ADATVÉDELMI TÁJÉKOZTATÓ MATRICA

**KAMERÁVAL
MEGFIGYELT TERÜLET**

**A MEGFIGYELT TERÜLETEN TARTÓZKODÁSÁVAL ÖN
BELEEGYEZÉSÉT ADJA AHHOZ, HOGY VIDEOFELVÉTELEN
RÖGZÍTSÜK UTAZÁS ALATTI TEVÉKENYSÉGÉTI**

A felvétel készítésének célja: a személyszállító vasúti jármű belterében a jármű, továbbá az utasok személyének, testi épségének és vagyontárgyainak védelme.

Az adatkezelés jogalapja: a személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény 8. §.

A rögzítő rendszert üzemelteti és a felvételt tárolja: MÁV-START Zrt.

A felvétel tárolásának időtartama: 15 nap.

A felvételt megismerheti: ha az utas hatósági eljárást kezdeményezett, akkor a bíróság, illetve az eljárásra illetékes más hatóság. Hatósági kikérés hiányában a felvétel a rögzítésétől számított 16. napon megtekintés nélkül törlésre kerül.

Az utas jogosult a vonaton a jegyvizsgálónál, vagy a vasútállomáson igényelhető Bejelentőlap kitöltésével a tárolási időn belül kérni, hogy a felvételt az üzemeltető a hatósági eljáráshoz őrizze meg. A kamerával rögzített személyes adatairól az alább olvasható elérhetőségeken a tárolási időn belül tájékoztatást kérhet, és kérheti azok törlését.

Figyelem: a felvétel megőrzésének kérése mellett az utasnak kell megtennie a rendőrségi feljelentést is úgy, hogy a felvétel hatósági kikérése a felvétel tárolási időtartamán belül megérkezessen az üzemeltetőhöz.



UTAZZON BIZTONSÁGBAN

» www.mav-start.hu

MÁVDIREKT: 06 (40) 49-49-49 (00:00-24:00 óráig helyi tarifával hívható kék szám) • költözőről: +36/1 444-4499
E-MAIL: információkérés informacio@mav-start.hu • jegy-, különvonat-, Diák-Charter-, csoportos utazások értékesítés mav-start.hu

25/2014. (II. 12. MÁV-START Ért. 9.) sz. vezérigazgatói utasítás a MÁV-START Zrt. Üzlettitok-védelmi Szabályzata

1.0 AZ UTASÍTÁS CÉLJA

Az utasítás célja a MÁV-START Zrt-nél (a továbbiakban: Társaság) az üzleti titok fogalmának, az abba tartozó adatok körének, az üzleti titokká minősítés eljárási rendjének, továbbá az üzleti titokká minősített adatok kezelésének, felhasználásának és védelmi szabályainak meghatározása a Polgári Törvénykönyvről szóló törvény (a továbbiakban: Ptk.) rendelkezéseivel összhangban.

2.0. HATÁLY ÉS FELELŐSSÉG MEGHATÁROZÁSA

2.1. Az utasítás hatálya

Az utasítás hatálya kiterjed a Társaság valamennyi szervezeti egységére és munkavállalójára, valamint a MÁV-START Zrt. Igazgatósága és MÁV-START Zrt. Felügyelő Bizottsága tagjaira, a két szervezet ügyrendjében szabályozott kiegészítésekkel és eltérésekkel.

2.2. Az utasítás kidolgozásáért és karbantartásáért felelős

Az utasítás kidolgozásáért és karbantartásáért a Biztonság vezetője felelős.

3.0. FOGALOMMEGHATÁROZÁSOK

3.1. Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek, vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

3.2 Adathordozó: a papír és azok a számítógépes alkatrészek, amelyekre a munkához szükséges adatokat menteni, tárolni lehet, illetve a hordozható változataikkal gép-gép között adateserét lehet megvalósítani, például:

- mágneses elven működő egységek (pl.: FDD, HDD, IBM Microdrive),
- az optikai adattárolás elvén működő adathordozók (pl.: CD, DVD, Blu-Ray Disc (BD)) memóriakártyák (pl.: Smart Media, Compact Flash, SDHC),
- USB, soros, IRDA portra csatlakoztatható eszközök (pl.: pen-drive, okostelefon, fényképezőgép, zenelejátszók, videokamerák).

3.3. Adatmegsemmisítés: az adatok, vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése.

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

3.5. Belső adat: a Társaság tevékenységéhez kapcsolódó olyan adat, amelynek a védelméhez méltányolható érdek fűződik, és nyilvánosságra kerülése sértené a Társaság érdekeit, de az üzleti titok kategóriába nem sorolható, annál kevésbé fontos tartalommal bír.

3.6. Betekintési engedély: a minősítő vagy a címzett által az üzleti titok megismerésére írásban adott felhatalmazás.

3.7. Betekintő: az a természetes személy, aki a betekintésre munkakörénél fogva jogosult, illetve akinek munkaköre ellátásához az üzleti titok megismerése szükséges, és a minősítő vagy a címzett feljogosította a szóban forgó adat megismerésére vagy kezelésére.

3.8. Címzett: az a természetes személy, akinek a minősítő rendelkezése alapján a dokumentum megküldésre került, vagy megküldhető.

3.9. Elektronikus dokumentum: elektronikus eszközzel készített, és azzal értelmezhető adat.

3.10. Érvényességi idő: az év, hó, nap szerint feltüntetett időpont, amelynek eléréséig a minősítési jelöléssel ellátott adat megismerését a jogszerű minősítés korlátozza.

3.11. Érzékeny adat: a személyes adat, a belső adat és a (titokká) minősített adat együttes elnevezése.

3.12. Illetéktelen személy: aki a minősített adat megismerésére nem jogosult.

3.13. Közérdekű adat: az állami vagy helyi önkormányzati feladatot valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől.

3.14. Közérdekből nyilvános adat: minden olyan természetes személy, jogi személy, vagy jogi személyiséggel nem rendelkező szervezet kezelésében lévő vagy rá vonatkozó,