54/2020. (III. 13. MÁV Ért. 10.) EVIG számú utasítás a MÁV Zrt. adatvédelmi és adatbiztonsági szabályzata

1.0 AZ UTASÍTÁS CÉLJA

Az adatvédelmi és adatbiztonsági szabályzat (utasítás) kiadásának célja a MÁV Zrt. (a továbbiakban: Társaság) tevékenységével összefüggésben a természetes személyek alapvető jogainak és szabadságainak a személyes adataik kezelése tekintetében megillető védelméhez fűződő jog érvényesülésének biztosítása, a Társaság által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása, a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírások meghatározása.

Jelen utasítás végrehajtása során biztosításra kerül a 2012/34/EU európai parlamenti és tanácsi irányelvnek a belföldi vasúti személyszállítási szolgáltatások piacának megnyitása és a vasúti infrastruktúra irányítása tekintetében történő módosításáról szóló 2016/2370/EU Európai Parlamenti és Tanácsi irányelv (4. vasúti csomag), a vasúti közlekedésről szóló 2005. évi CLXXXIII. törvény, a pályahálózat-működtető függetlenségének feltételeiről szóló 11/2019. (V.29.) ITM rendeletben előírt informatikai, adatkezelési rendszerek elkülönítésének betartása.

A szabályozás különösen az alábbi jogszabályokra, ajánlásokra és irányelvekre, belső szabályozásokra alapozva, azokkal teljes összhangban került kialakításra:

- Magyarország Alaptörvényének VI. cikke;
- az Európai Parlament és Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: általános adatvédelmi rendelet) (angolul: General Data Protection Regulation, röviden: GDPR);
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.);
- Az Európai Parlament és a Tanács 1370/2007/EK Rendelete (2007. október 23.) a vasúti és közúti személyszállítási közszolgáltatásról, valamint az 1191/69/EGK és az 1107/70/EGK tanácsi rendelet hatályon kívül helyezéséről;
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.);
- a személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény (a továbbiakban: Szsztv.);
- a személy és vagyonvédelmi, valamint magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban Szvmt.);
- a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.);
- az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.);
- a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvény;
- a fogyasztóvédelemről szóló 1997. évi CLV. törvény (a továbbiakban: Fgytv.);
- a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény;
- a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról szóló 1997. évi CLIX. törvény (a továbbiakban: Fbőtv.);
- a minősített adat védelméről szóló 2009. évi CLV. törvény;
- a pénzmosás és terrorizmus finanszírozása megelőlegezéséről és megakadályozásáról szóló 2017. évi LIII. törvény.

E szabályzatnak nem célja a személyes adatok kezelése tekintetében, azok védelmét érintően kiadott EU rendeletek, irányelvek és más jogi aktusok, hazai jogszabályok, felügyeleti hatósági ajánlások teljes körű átvétele, megismétlése. A személyes adatok jogszerű kezelése érdekében ezért a szabályzat mellett a jogi környezetet átfogóan kell megismerni és alkalmazni, a belső szabályozással való esetleges ellentmondás esetén a kötelező érvényű jogi előírásokat kell irányadónak tekinteni. Az

adott adatkezelésre vonatkoztatható Európai Adatvédelmi Testület (European Data Protection Board – EDPB) vagy felügyeleti hatósági ajánlások, állásfoglalások, iránymutatások, legjobb gyakorlatok közvetlen alkalmazása tekintetében indokolt a Társaság adatvédelmi tisztviselője tanácsát kikérni.

2.0 HATÁLY- ÉS FELELŐSSÉG MEGHATÁROZÁSA

2.1 Személyi hatály

A szabályzat személyi hatálya kiterjed a Társaság valamennyi adatkezelőként, adatfeldolgozóként adatkezelési tevékenységet ellátó, illetve abban közreműködő szervezeti egységére, munkavállalójára, valamint a Társasággal szerződéses jogviszonyban álló természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre, a velük kötött polgári jogi szerződés vagy adatkezelési feladatokra vonatkozó megállapodás alapján, amennyiben az érintett jogviszonyban magukra nézve kötelezően elfogadták jelen szabályzat hatályát.

2.2 Tárgyi hatály

Tárgyi hatálya kiterjed a Társaság szervezeti egységeinél történő valamennyi személyes adat részben vagy egészben automatizált módon történő elektronikus, valamint manuális kezelésre, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni, beleértve a papíralapú, valamint a nyilvántartásba nem rendezett adatkezeléseket is. Nem kell az utasítás rendelkezéseit alkalmazni a munkavállalók kizárólag saját személyes céljaikat szolgáló adatkezeléseire, valamint a közérdekű adatok megismerésének szabályaira. A közérdekből nyilvános adatokkal összefüggésben a Társaság Közzétételi szabályzatáról szóló utasításban foglalt előírások, informatikai adatbiztonsággal összefüggő kérdésekben a Társaság Informatikai biztonsági szabályzatáról szóló utasítás (a továbbiakban: IBSZ) az irányadó.

2.3 Az utasítás kidolgozásáért és karbantartásáért felelős

A Biztonsági főigazgatóság vezetője gondoskodik ezen szabályzat elkészítéséről és szükség szerinti módosításáról.

3.0 FOGALMAK MEGHATÁROZÁSA

A szabályzat alkalmazása során – összhangban az általános adatvédelmi rendelettel, valamint az Mt. előírásaival – a következőkben meghatározott fogalmak irányadók:

adatállomány: az egy nyilvántartásban kezelt adatok összessége;

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;

adatbiztonság: az informatikai (adattároló és feldolgozó) rendszer azon állapota, amelyben az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának kockázata megelőző intézkedésekkel elviselhető mértékűre csökkenthető. Ez az állapot az EU kötelező jogi aktusain, jogszabályokon, nemzetközi szabványokon alapuló előírások és megelőző biztonsági intézkedések betartásának eredménye;

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

adathordozó: azon eszközök (pl. merevlemezek, szalagok, kazetták, flash memória alapú tárolóeszközök) összefoglaló neve, amelyek az adatok digitális formában történő tárolására szolgál;

adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

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

adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

adatszivárgás elleni védelmi rendszer (Data Loss Prevention, röviden DLP): olyan informatikai védelmi rendszer, amely a technikai lehetőségek és beállítások határán belül észleli, jelzi, illetve megakadályozza a védendő információ jogosulatlan használatát, továbbítását a végpontok, a hálózat és az adathordozók tekintetében egyaránt;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele. Az adatkezelő vagy adatfeldolgozó abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre;

adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

adatvédelem: a személyes adat jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége;

adatvédelmi kapcsolattartó: a Társaság adatkezelője által megbízott, az adatvédelmi ismeretek terén kellő tájékozottsággal rendelkező munkavállaló, aki részt vesz az adatkezelést érintő feladatok végrehajtásában és kapcsolatot tart az adatvédelmi tisztviselővel, illetve az adatvédelmi szakértőkkel;

adatvédelmi szakértő: a Biztonsági főigazgatóság Információ- és adatvédelem szervezetének informatikai biztonsági, illetve adatvédelmi ismeretekkel rendelkező szakértője;

adatvédelmi tisztviselő: az általános adatvédelmi rendelet 37. cikk. (1) a) alapján a Társaság, mint köz-feladatot ellátó szervezet köteles adatvédelmi tisztviselőt kijelölni. A Társaság elnök-vezérigazgatója a 37. cikk. (5) értelmében a szakmai rátermettség, az adatvédelmi jog és gyakorlat szakértői szintű ismere-te, valamint az ezzel összefüggő feladatok ellátására való alkalmassága alapján a Biztonsági főigazgatóság Információ- és adatvédelem szervezet munkavállalói közül írásban jelöli ki a megfelelő személyt.

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;

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

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

bűnügyi személyes adat: a büntetőeljárás 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;

címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek;

cookie (süti): rövid adatfájl, amelyet a meglátogatott honlap helyez el a felhasználó számítógépén, abból a célból, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolható. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl. egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Tekintve, hogy a cookie segítségével nyomon követhetők a felhasználó böngészési szokásai, ezért azt kizárólag a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni;

döntés megalapozását szolgáló adat: a Társaság, mint közfeladatot ellátó szerv feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló adat (ilyen adat például a belső használatra szánt munkaanyag, emlékeztető, tervezet, vázlat, javaslat, a Társaságon belül váltott levelek, általában a döntés-előkészítés körében alkotott iratok, amelyek nyilvánosságra hozatala jelentősen hátráltathatja a munkavállalókat feladataik teljesítésében, vagy a társaság számára hátrányt jelent);

drón (távolról irányított légi jármű)**:** egy távolról irányított repülő eszközből, valamint arra felszerelhető, konfigurálható eszközökből (pl. kamera, mikrofon), a szükséges irányító, vezérlő egységekből és egyéb, a repüléshez szükséges eszközökből áll;

elektronikus biztonságtechnikai rendszer: egy vagy több képérzékelőből, rögzítőből, illetve megjelenítőből álló, meghatározott terület figyelésére, illetve az ott észleltek rögzítésére alkalmas eszköz, amely további rendszerekhez is kapcsolódhat, illetve bővíthető egyéb elemekkel (mozgásérzékelő, fényvető stb.). A rögzített adatok vezetékes, vagy vezeték nélküli kapcsolaton keresztül továbbíthatók, illetve külső adathordozóra is kimenthetők. Asztali, illetve hordozható számítógépről (pl. okostelefon, tablet), a megfelelő védelmi intézkedések betartása mellett, az erre feljogosított felhasználók számára biztosíthatja, hogy a rendszerbe számítógépes hálózat, illetve az internet segítségével akár távolról is be lehessen lépni, meg lehessen tekinteni az aktuális élőképeket, vezérelni lehessen a mozgatható kamerákat, programozni azok képérzékelő képességét, illetve az adatbázisból elő lehessen hívni az ott tárolt felvételeket;

érintett: azonosított vagy azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítani lehet;

felügyeleti hatóság: az általános adatvédelmi rendeletben a felügyeleti hatóság részére megállapított feladat- és hatásköröket gyakorló, Magyarországon az Infotv.-ben meghatározott Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban NAIH, vagy Hatóság);

forgalomtechnikai kommunikációs eszközök: diszpécsertelefon, mozdonyrádió, GSM-R rádiótelefon, egyéb üzemviteli kommunikációs eszköz;

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

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

IHIR: Integrált Humán Irányítási Rendszer;

informatikai eszköz (IBSZ szerint)**:** bármely feladat ellátására létrehozott, informatikai technológia felhasználásával működtetett (pl. vezérelt) telepített, vagy mobil eszközök, továbbá rendszerek,

eljárások összessége vagy ezek alkotó elemei (pl. asztali vagy hordozható számítógép, adathordozó, nyomtató, operációs rendszer, felhasználói programok [irodai alkalmazások, adatbáziskezelő, vezérlő programok, beágyazott informatikai rendszerek és egyéb egyedi fejlesztésű célprogramok stb.], továbbá az informatikai alapokra épülő távközlési rendszerek [pl. IP telefon rendszer és végberendezései, hálózati aktív és passzív eszközök], valamint a hálózatmenedzsment elemei);

kötelező adatkezelés: az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez, vagy a közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladata végrehajtásához szükséges adatkezelés, amelyek esetében a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg;

közérdekből nyilvános adat: a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízása, a közfeladat ellátásával összefüggő egyéb személyes adata, valamint azok a személyes adatai, amelyek megismerhetőségét törvény előírja;

közterület: a közhasználatra szolgáló minden olyan állami vagy önkormányzati tulajdonban álló terület, amelyet rendeltetésének megfelelően bárki használhat, ideértve a közterületnek közútként szolgáló és a magánterületnek a közforgalom számára a tulajdonos (használó) által megnyitott és kijelölt részét, továbbá az a magánterület, amelyet azonos feltételekkel bárki használhat;

különleges adatok: A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;

MÁV-csoport: a MÁV Zrt. SZMSZ I. kötete 6.5.1.2. pontjában meghatározott társaságok;

megfelelő tájékoztatás: az érintettel az adatkezelés megkezdése előtt közölni kell az adatkezelés jogalapját, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen a kezelt adatok köréről, az adatkezelés céljáról és jogalapjáról, az adatkezelő és az adatfeldolgozó személyéről, az adatkezelés időtartamáról, illetve az adattovábbítás címzettjéről. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is;

minősített adat (nemzeti minősített adat): a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést törvényben, valamint törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti, és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;

Mobil Device Management (MDM): mobil kommunikációs képességekkel rendelkező infokommunikációs eszközökre (pl. okostelefonokra, tabletekre) telepített felügyeleti rendszer, amely biztosítja az eszközök távoli felügyeletét, a tárolt adatok, programok és szolgáltatások védelmét;

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH): lásd: Felügyeleti hatóság;

nyilvánosságra hozatal: az adat bárki számára hozzáférhetővé tétele;

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

profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz,

személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

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

személyes adatok különleges kategóriái: lásd: különleges adat;

személyszállítási közszolgáltatás: a nyilvánosság számára megkülönböztetés nélkül és folyamatosan nyújtott általános gazdasági érdekű személyszállítási szolgáltatások (az 1370/2007/EK rendelet 2. cikk a) pontja szerinti, közszolgáltatási szerződés alapján végzett személyszállítási szolgáltatás);

személyszállítási közszolgáltató: bármely társaság, vagy vállalatcsoport tagja, amely személyszállítási közszolgáltatásokat működtet, vagy bármely olyan közjogi szerv, amely személyszállítási közszolgáltatásokat nyújt;

távolról végzett munka: a Társaság informatikai rendszerének biztonsági zónáján kívül eső (nem védett) környezetből végzett tevékenység, amely során a Társaság a felhasználó számára olyan informatikai erőforrások elérését biztosítja (jellemzően VPN-en keresztül), amellyel a munkahelyén egyébként rendelkezhet. Ide nem értendők azoknak a technológiáknak, illetve mobil informatikai megoldásoknak alkalmi felhasználása, amellyel eseti információcserét lehet megvalósítani (pl. OWA, Push email, OAW);

területi adatvédelmi szakértő: a Biztonsági főigazgatóság Területi vasútbiztonság szervezet – az adatvédelmi tisztviselő előzetes egyetértésével – írásban megbízott munkavállalója, aki az adott szakterületen szerzett átfogó helyismeret mellett informatikai biztonsági, valamint adatvédelmi ismeretek terén is kellő tájékozottsággal rendelkezik. A területi adatvédelmi szakértő munkahelyi vezetője irányításával, az adatvédelmi tisztviselő szakmai felügyelete mellett segíti elő az adatvédelmi előírások érvényesülését;

tiltakozás: az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében, illetve jogos érdekeinek érvényesítésén alapuló kezelése ellen;

törzsszám: a Társaság munkavállalóját az adatkezelés során egyértelműen azonosító, az IHIR rendszerben képzett, belső azonosítási célokat szolgáló számjegysor;

üzleti titok: a gazdasági tevékenységhez kapcsolódó, titkos – egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető –, ennél fogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja;

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);

védendő információ: a jogszabályi védelem alatt álló minősített adat, az üzleti titok, a védett ismeret (know-how), a személyes adat, a Társaság feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, döntés vagy további jövőbeli döntés megalapozását szolgáló nem nyilvános adat, továbbá a munkakör betöltésével összefüggésben a munkavállaló tudomására jutott egyéb információ, amelynek felfedése, közlése a munkáltató, vagy más személy számára hátrányos következményeket hordozhat; ezeken túl a Társaság által kezelt azon adatok is, amelyek bizalmasságához, sértetlenségéhez, rendelkezésre állásához a Társaságnak jogos érdeke fűződik, kivéve, ha a nyilvánosságra hozatalt jogszabály, vagy belső utasítás írja elő, teszi lehetővé, illetve azt az arra jogosult korábban már nyilvánosságra hozta;

védett ismeret: (know-how) üzleti titoknak minősülő, azonosításra alkalmas módon rögzített, műszaki, gazdasági vagy szervezési ismeret, megoldás, tapasztalat vagy ezek összeállítása;

VPN (Virtual Private Network – virtuális magánhálózat): A VPN alkalmazása lehetővé teszi a felhasználók számára, hogy egy megosztott vagy nyilvános hálózaton keresztül úgy küldjenek és fogadjanak adatokat, mintha számítógépeik közvetlenül kapcsolódnának a helyi hálózathoz. A VPN egy gyakori alkalmazása, amikor a munkavállalók távolról biztonságosan, az interneten keresztül férhetnek hozzá a Társaság belső hálózatához a felhasználó számítógépe és a Társaság szervere között létrehozott titkosított csatorna segítségével;

„Zártan kezelendő!": a személyes adatot tartalmazó dokumentumok általános védelmi előírása. Amennyiben az adathordozóról nem állapítható meg egyértelműen adattartalmának védendő jellege, vagy az adatkezelő a hozzáférési jogosultságok betartása érdekében külön ki kívánja emelni a kezelés zártságának követelményét, abban az esetben ezt kezelési utasításként kell ezt a dokumentumon feltüntetni.

4.0 AZ UTASITÁS LEÍRÁSA

4.1 A személyes adatok védelme

4.1.1 Az adatkezelés elvei

A Társaságnál a személyes adatok kezelését jogszerűen, tisztességes eljárásban, átlátható módon, célhoz kötötten kell végrehajtani. Ennek során tekintettel kell lenni az adattakarékosság elvére, az adatok korlátozott tárolhatóságára, bizalmasságára és integritására, egyúttal gondoskodni kell az adatok pontosságáról.

Ennek megfelelően a személyes adatok:

a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;
b) gyűjtésük csak meghatározott, egyértelmű és jogszerű célból történhet, nem kezelhetők ezen célokkal össze nem egyeztethető módon;
c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükséges minimumra kell korlátozódniuk;
d) pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalanul törlésre vagy helyesbítésre kerüljenek;
e) tárolásuknak olyan formában kell megtörténnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;
f) megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát, beleértve az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is.

Az adatkezelőnek azon túl, hogy felelős ezen elveknek történő megfelelésért, képesnek is kell lennie a megfelelés igazolására. E pontban leírtakra vonatkozóan az adatkezelő elszámoltathatóságára tekintettel kell a részletes dokumentálást elkészíteni.

4.1.2 Az adatkezelés jogalapja

Az adatkezelés jogalapjait az általános adatvédelmi rendelet tartalmazza, melyek a következők:

a) az érintett hozzájárulása;
b) az érintettel létesített vagy létesítendő szerződéses viszony;
c) az adatkezelőre vonatkozó jogi kötelezettség teljesítése;
d) az érintett vagy más természetes személy létfontosságú érdeke;
e) közérdekű feladat ellátása és közhatalomi jogosítvány gyakorlása;
f) az adatkezelő vagy harmadik fél jogos érdeke.

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

adatok kezeléséhez. A hozzájárulásnak megfelelő előzetes tájékoztatáson, az önkéntességen, illetve a hozzájárulás akaratának konkrét és egyértelmű kinyilvánításán kell alapulnia. Adatkezelő a hozzájárulás jogalapjára nem hivatkozhat jogszerűen, amennyiben ezen elemek közül valamelyik nem felel meg a rájuk vonatkozó követelményeknek. A tájékoztatásnak érthetőnek, kellően részletesnek, pontosnak és világosnak kell lennie.
Tizennyolc éven aluli személy esetében a törvényes képviselőjének hozzájárulása szükséges.
Hozzájárulást sokféleképpen meg lehet adni, például, ha az érintett valamely internetes honlapon bejelöl egy erre vonatkozó négyzetet vagy ha az érintett megfelelő technikai beállításokat hajt végre. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.
A hozzájárulás jogszerűségét az adatkezelőnek bizonyítania kell tudnia, azonban nem szolgálhat érvényes jogalapként a személyes adatok kezeléséhez olyan egyedi esetekben, amelyekben az adatkezelő és az érintett között egyértelműen egyenlőtlen viszony áll fenn (pl. munkaadó-munkavállaló viszony), és ezért az adott helyzet valamennyi körülményét figyelembe véve valószínűtlen, hogy a szóban forgó hozzájárulás megadása önkéntesen történik.
Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja, azonban ez nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását. A hozzájárulás visszavonhatósága is mutatja, hogy olyan esetekben, amikor más jogalap is rendelkezésre áll, akkor azt kell használni, hiszen ellenkező esetben a hozzájárulás visszavonása miatt lehetetlenné válik a további adatkezelés vagy a visszavonásra tekintettel más jogalapra helyezkedés az egész addigi adatkezelés jogszerűségét megkérdőjelezi.

A szerződéses viszonyon alapuló adatkezelés szerint jogszerű az az adatkezelés, amely olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges. Ez a jogalap két esetben alkalmazható. Akkor, ha az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, valamint, amennyiben az adatkezelés a szerződés megkötését megelőzően bizonyos lépéseknek az érintett kérésére történő megtételéhez szükséges. A szerződés teljesítéséhez szükséges adatkezelés előfeltétele egy olyan érvényes szerződés, amelyben az egyik szerződő fél az érintett. Ilyen lehet például a munkaszerződés, amelyben a munkáltatónak a szerződés teljesítéséhez szükséges a munkavállalók adatait kezelnie. A munkaviszonyból eredően azonban további adatkezelések, adatkezelési célok is keletkeznek, keletkezhetnek, amelyek vonatkozásában azonban a szerződés jogalapja helyett más jogalapok, például a jogi kötelezettség vagy a jogos érdek alkalmazható. A szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges adatkezelés az, amikor a felek között még nem jött létre szerződés, azonban ahhoz, hogy ez megtörténjen, bizonyos olyan lépéseket kell megtenni, amelyekhez szükséges adatkezelés. Ezen megelőző lépésekre az érintett, és nem az adatkezelő vagy egy harmadik fél érdekében, illetve kezdeményezésére kerülhet sor (pl. munkaszerződés előkészítése).

Jogi kötelezettség teljesítése esetén az adatkezelés alapvető követelményeit elsősorban törvény állapítja meg. Az adatkezelő jogi kötelezettségként az uniós jog által előírt jogi kötelezettségeket, valamint azokat a törvényi rendelkezéseket veheti figyelembe, amelyek esetében a törvény elrendeli az adatkezelést, és meghatározza annak alapvető körülményeit is. Abban az esetben, amikor a jogszabály csak általános felhatalmazást határoz meg a személyes adatok kezelésével járó tevékenység végzésére (például az Mt. azon rendelkezése, amely alapján a munkáltató a munkavállalót a munkaviszonnyal összefüggő magatartása körében ellenőrizheti) a törvény mindössze az ellenőrzés lehetőségét és nem kötelezettségét biztosítja. Ilyen esetben az adatkezelést valamely eltérő a jogalap alapján (pl. a munkáltató jogos érdeke alapján) kell megvalósítani.

Amennyiben jogszabály olyan jogi kötelezettséget ír elő, amely bár személyes adatok kezelésével jár, de az adott jogszabály nem határozza meg az adatkezelés körülményeit, úgy az adatkezelőnek kell érvényre juttatnia a személyes adatok kezelésére irányadó általános adatvédelmi rendelet szabályai szerinti alapelveket és garanciákat.

A **közfeladat ellátása** és a közhatalmi jogosítvány gyakorlása esetében jogszabály ruházza fel ezeket a szerveket közhatalmi jogosítványokkal, illetve ír elő számunka konkrét közfeladatokat. A GDPR

nem követeli meg, hogy az egyes konkrét adatkezelési műveletekre külön-külön jogszabály vonatkozzon, elegendő az is, ha egyetlen jogszabály szolgál jogalapul több olyan adatkezelési művelethez is, amely az adatkezelőre vonatkozó jogi kötelezettségen alapul, illetve amelyre közérdekből végzett feladat ellátásához vagy közhatalmi jogosítvány gyakorlásához van szükség. A MÁV Zrt., mint közfeladatot ellátó szerv minden közjogi és magánjogi jogviszonyának, és az ahhoz járulékosan kapcsolódó adatkezelési jogviszonyainak kizárólag közfeladatai ellátásával összefüggésben lehet alanya. A Társaság közfeladatait meghatározó jogszabályi rendelkezéseken alapuló adatkezelések jogalapja ezért a GDPR 6. cikk (1) bekezdés e) pontja.

A társaság közfeladatait az alábbi jogszabályok, szerződések határozzák meg:
- a vasúti közlekedésről szóló 2005. évi CLXXXIII. törvény 3/B §-a, illetve az az alapján megkötött pályaműködtetési szerződés;
- A Magyar Állam tulajdonosi joggyakorlója és a Társaság között fennálló érvényes vagyonkezelési szerződés.

Ha a jogalkotó ezen adatkezelésekre vonatkozó részletes szabályokat nem rögzítette, az adatkezelő az általános adatvédelmi szabályok – így különösen az alapelvek és a jogalap szükségességi mércéje – szerint köteles adatkezelési tevékenységét végezni, és annak jogszerűségét az elszámoltathatóság elvének megfelelően igazolni.

Más természetes személy **létfontosságú érdekeire** hivatkozással személyesadat-kezelésre különösen akkor kerülhet sor, ha az adatkezelésre humanitárius okokból – többek között járványok és terjedéseik nyomon követéséhez, vagy humanitárius vészhelyzetben, különösen természeti vagy ember által okozott katasztrófák esetében – van szükség.

Amennyiben **az adatkezelő jogos érdeke** szolgál az adatkezelés jogalapjául, az adatkezelés megkezdése előtt el kell készítenie egy ún. érdekmérlegelési tesztet. A tesztben az adatkezelőnek elemeznie kell például, hogy el lehet-e érni az adatkezelés célját személyes adatok kezelése nélkül, vagy kevesebb személyes adat kezelésével, mi az adatkezelő pontos célja és érdeke, mit hozhatnak fel az érintettek az adatkezeléssel szemben jogaik és szabadságaik védelmében, miért magasabb rendű az adatkezelő jogos érdeke, mint az érintettek érdekei. Amennyiben a tesztben megállapítást nyer, hogy az adatkezelő jogos érdekei megelőzik az érintettek érdekeit, akkor azt követően, hogy teljes körűen tájékoztatták az érintetteket az adatkezelésről és az érdekmérlegelési tesztről megkezdhető az adatkezelés.

Bizonyos típusú személyes adatok kezeléséhez még szigorúbb feltételek kapcsolódnak. Ezek **a személyes adatok különleges kategóriái**, olyan érzékeny adatok, amelyek védelméhez fokozott egyéni és társadalmi érdekek kapcsolódnak. Főszabály szerint az adatok különleges kategóriáinak kezelése tilos, de az általános adatvédelmi rendelet bizonyos esetekben kivételt tesz lehetővé. A személyes adatok különleges kategóriáira vonatkozó adatok kizárólag az érintett kifejezett hozzájárulásával, illetve az általános adatvédelmi rendelet által meghatározott kivételes esetekben kezelhetők, különösen, ha azt az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy hazai jog, illetve kollektív szerződés lehetővé teszi.

4.1.3 Személyes adatokat tartalmazó adatbázis kialakítása

Az adatvédelmi és adatbiztonsági intézkedések betartásának, valamint jelen szabályzat rendelkezései érvényesülése érdekében egy személyes adatokat tartalmazó adatbázis kialakítása során a leendő adatkezelést végző szervezet vezetőjének irányításával a következő lépéseket kell végrehajtani (a folyamat ábrája a 7.13 számú mellékletben található):

1) az adatkezelés koncepciójának megfogalmazása,
2) adatkezelés megnevezése
3) az adatkezelési tevékenységet végző szervezeti egység kijelölése
4) a kapcsolattartó munkavállaló kijelölése
5) az adatvédelmi tisztviselő előzetes tájékoztatása, szükség szerinti bevonása
6) az adatkezelés céljának meghatározása
7) az adatkezelés jogalapjának meghatározása

8) a feldolgozandó adatkör meghatározása (az adatminimalizálás elvének alkalmazása)
9) álnevesítés, anonimizálás lehetőségének vizsgálata
10) annak vizsgálata, hogy különleges személyes adatok feldolgozására kerül-e sor
11) az adatkezeléssel érintettek csoportjának leírása, várható számosságának behatárolása
12) adatok forrásának meghatározása
13) adatok átvétele esetén a jogalap tisztázása, módja
14) ha az adatkezelés a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal jár, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot hajt végre, amelynek során köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát
15) ha a hatásvizsgálat azt állapítja meg, hogy az adatkezelés – az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában, vagy azok mellett – valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatvédelmi tisztviselő konzultációt kezdeményez a felügyeleti hatósággal
16) az adatkezelés technológiájának, illetve automatizáltságának kiválasztása
17) az adatvédelmi incidens detektálásának, kezelésének módja
18) adatvédelmi incidenst követően – szükség esetén – az érintettek tájékoztatásának megtervezése
19) informatikai feldolgozó rendszer alkalmazása esetén az IBSZ, valamint a rendszerszintű informatikai biztonsági szabályzatok előírásainak érvényesítése
20) adatfeldolgozó, illetve további adatkezelő bevonása esetén megállapodás készítése
21) a tényleges adatkezelés helyének meghatározása
22) adattovábbítás esetén a továbbítandó adatok körének meghatározása, jogalapjának kiválasztása, a címzett meghatározása
23) az adatok korlátozásának, kiadásának, törlésének és archiválásának megtervezése
24) szükség szerint adatkezelési szabályzat elkészítése
25) az adatkezelés bejelentése az adatkezelési nyilvántartásba (7.5 számú melléklet)
26) amennyiben a rendszer munkavállalók technikai ellenőrzésére szolgál, az alkalmazott eljárás részleteit külön fejezetben kell megjeleníteni
27) az adatkezelési tájékoztató és a hozzájáruló, illetve adatvédelmi nyilatkozat elkészítése
28) szükség esetén adatvédelmi audit adatkezelő általi kérése
29) üzemi tanács véleményének kikérése, amennyiben a munkavállalók nagyobb csoportját érinti a bevezetendő technikai ellenőrzés
30) a nyilvántartásba vételt követően – szükség szerint – az adatkezeléshez történő hozzájárulások beszerzése, a dokumentumokon a nyilvántartási szám feltüntetése, majd az adatkezelés megkezdése.

Az adatkezelő vagy adatfeldolgozó – különösen kockázatosnak ítélt adatkezelés esetén – kérheti, hogy a felügyeleti hatóság vagy tanúsító szervezet adatvédelmi tanúsítási eljárás során igazolja, hogy az általa végrehajtott adatkezelési műveletek megfelelnek az általános adatvédelmi rendelet előírásainak.

4.2 Az adatkezelésben közreműködők és feladataik

4.2.1 A Társaság elnök-vezérigazgatója

Kijelöli és ezzel a feladattal megbízza az adatvédelmi tisztviselői feladatokat ellátó személyt.

4.2.2 Biztonsági főigazgató

Az Információ- és adatvédelem szervezet vezetője útján irányítja és ellenőrzi az adatvédelemmel kapcsolatos feladatok végrehajtását. Ennek során jóváhagyja az adatvédelmi ellenőrzési tervet, illetve elfogadja az erről készített jelentést. Indokolt esetben tájékoztatja a Társaság elnök-vezérigazgatóját, illetve az intézkedések végrehajtását kezdeményezi az illetékes főtevékenységi kör vezetőnél. Gondoskodik a jelen szabályzat aktualizálásáról.

4.2.3 Főtevékenységi kör vezető

Biztosítja az adatvédelmi tisztviselő számára a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon, így különösen az ilyen tárgyú vagy kapcsolódású utasítások és előterjesztések véleményezése útján, továbbá az irányítása alá tartozó, természetes

személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal járó adatkezelés vonatkozásában kötelező érvénnyel intézkedik az adatvédelmi tisztviselő tanácsának kikérésre.

4.2.4 Adatvédelmi tisztviselő

Az adatvédelmi tisztviselő e feladatkörében a biztonsági főigazgató útján a Társaság elnök-vezérigazgatójának tartozik felelősséggel; e tevékenységével összefüggésben utasításokat nem fogadhat el, nem bocsátható el és szankcióval nem sújtható. Amennyiben más feladatokat is ellát, gondoskodni kell az összeférhetetlenség elkerüléséről. Az érintettek a személyes adatok kezelésével összefüggő kérdésekben közvetlenül fordulhatnak hozzá.

4.2.4.1 Az adatvédelmi tisztviselő kijelölése

A Társaság elnök-vezérigazgatója szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint az általános adatvédelmi rendeletben meghatározott feladatok ellátására való alkalmasság alapján az Információ- és adatvédelem szervezet állományából adatvédelmi tisztviselőt jelöl ki. Kizárólag olyan személy jelölhető ki adatvédelmi tisztviselőnek, akinek nincs olyan Ptk. szerinti hozzátartozója, aki a Társaságnál adatkezeléssel kapcsolatos döntések meghozatalára jogosult. Az adatvédelmi tisztviselő más feladatokat is elláthat, de a Társaság a Szervezeti és működési szabályzatában, valamint a munkaköri leírás útján biztosítja számára, hogy ezekből a feladatokból ne keletkezzen összeférhetetlenség, valamint egyéb munkaköri feladatainak ellátása ne veszélyeztethesse az adatvédelmi tisztviselői feladatai ellátását. Az adatvédelmi tisztviselő kinevezése határozatlan időre szól, az elérhetőségeit közzé kell tenni a Társaság honlapján és azt egyúttal közölni kell a felügyeleti hatósággal is.

4.2.4.2 Az adatvédelmi tisztviselő jogállása

a) a Társaság valamennyi adatkezelést végző szervezet vezetője biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos ügyekbe megfelelő módon és időben bekapcsolódjon;

b) a biztonsági főigazgató támogatja az adatvédelmi tisztviselőt a feladatai ellátásában azáltal, hogy biztosítja számára azokat a forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek;

c) jelen szabályzat, valamint az adatvédelmi tisztviselő részére kiadott kijelölő dokumentum és Munkaköri leírás alapján biztosítja, hogy a 4.2.4.3 pontban meghatározott feladatai ellátásával kapcsolatban senkitől ne fogadjon el utasításokat. Az adatvédelmi tisztviselő közvetlenül a Társaság legfelső vezetésének tartozik felelősséggel, feladatai ellátásával összefüggésben a munkáltató részéről közölt sem rendes sem azonnali hatályú felmondással munkaviszonya nem szüntethető meg és szankcióval sem sújtható;

d) a minősített adatok védelméről szóló törvény alapján kinevezett biztonsági vezető útján biztosítja az adatvédelmi tisztviselő számára feladatainak ellátása céljából, az ahhoz szükséges mértékben a minősítéssel védett iratokba történő betekintést, és az ennek jogszerű gyakorlásához szükséges személyi biztonsági feltételeknek történő megfelelést;

e) elkülönített, közvetlen e-mail címet és üzemi telefonszámot biztosít az adatvédelmi tisztviselő számára, ezáltal is biztosítva számára annak lehetőségét, hogy a személyes adatok kezelésével érintettek, a Társaság bármely munkavállalója közvetlenül és egyszerű módon fordulhasson hozzá.

Az adatvédelmi tisztviselő jogviszonyának fennállása alatt és annak megszűnését követően is titokként köteles megőrizni a tevékenységével, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni.

Az adatvédelmi tisztviselő részt vesz a felügyeleti hatóság által összehívott adatvédelmi tisztviselők konferenciáján.

Az adatkezelő, az adatfeldolgozó, valamint bármely munkavállaló a szolgálati út igénybevétele nélkül közvetlenül konzultálhat az adatvédelmi tisztviselővel az adatvédelmi szabályok értelmezésével vagy alkalmazásával kapcsolatos bármely kérdésről. Az adatkezeléssel érintettek a személyes adataik kezelésével kapcsolatosan és az általános adatvédelmi rendelet szerinti jogaik gyakorlása érdekében közvetlenül fordulhatnak az adatvédelmi tisztviselőhöz. Senkit sem érhet hátrány amiatt, hogy olyan információt hoz az adatvédelmi tisztviselő tudomására, amely megítélése szerint az adatvédelmi rendelkezéseket sérti.

Az adatvédelmi tisztviselő távolléte esetére helyettesítő személy kijelölése és részére feladat-meghatározás útján gondoskodik a 4.2.4.3 pontban felsorolt feladatai ellátásáról. Ilyen rendelkezés hiányában az elnök-vezérigazgató jogosult a helyettesítő személyének írásban történő megbízással való kijelölésére. Az adatvédelmi tisztviselő tartós távolléte (3 hónapot meghaladó időtartam) esetén a helyettesítéssel megbízott személy gondoskodik az adatvédelmi tisztviselő nevének és elérhetőségének a NAIH számára történő bejelentéséről.

4.2.4.3 Az adatvédelmi tisztviselő feladatai

a) tájékoztat és tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző munkavállalók részére az adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
b) független módon biztosítja az adatvédelmi szabályok belső alkalmazását; ellenőrzi az általános adatvédelmi rendeletnek, valamint az egyéb alkalmazandó, adatvédelmi rendelkezéseket tartalmazó jogszabályoknak, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
c) gondoskodik arról, hogy az érintetteket tájékoztassák az adatvédelemmel összefüggő jogaikról és kötelezettségeikről;
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, ha az adatvédelmi hatásvizsgálat azt állapítja meg, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések ellenére valószínűsíthetően magas kockázattal jár;
e) kérésre tanácsot ad a felügyeleti hatósággal történő előzetes konzultáció szükségessége tekintetében, amennyiben kétség merül fel annak indokoltságával kapcsolatban;
f) az adatkezelésért felelős szerv vezetőjével együttműködve válaszol a felügyeleti hatóság hozzá intézett megkeresésére;
g) gondoskodik az érintettek jogai érvényesítése érdekében hozzá benyújtott megkeresések kezeléséről;
h) vezeti az Adatvédelmi Munkacsoportot és összehívja a MÁV-csoport Adatvédelmi tisztviselők egyeztető fórumát;
i) az adatvédelmi kérdésekkel összefüggésben az *adatvedelem@mav.hu* e-mail címen, illetve a 01/24-00 telefonszámon fogadja Társaság munkavállalóinak, illetve szerződéses partnereinek megkeresését, konzultációs kérdéseit és azzal érdemben foglakozik.

4.2.5 Az információ- és adatvédelem szervezet vezetője

a) javaslatot tesz adatvédelmi ellenőrzési terv elkészítésére, részt vesz az ellenőrzés lefolytatásában, valamint a Vizsgálati jelentés összeállításában;
a) gondoskodik az adatkezelési nyilvántartásban az adatok aktualizálásáról;
b) gondoskodik az adatvédelmi incidens nyilvántartás vezetéséről;
c) gondoskodik a Társaság adatvédelmi és adatbiztonsági szabályzatának előkészítéséről és aktualizálásáról;
d) ellenőrzi a munkahelyeken, a számítógépeken, elektronikus adathordozókon a személyes adatok, illetve ezek felhasználásával készült elektronikus és papíralapú dokumentumok kezelését, azok megfelelő tárolását;

e) közreműködik az adatvédelmi tisztviselő feladatainak ellátásában;
f) részt vesz az adatvédelemmel összefüggően bekövetkezett incidensek kivizsgálásában;
g) szakmai segítséget nyújt az adatkezelő szervezeti egységek részére;
h) az információvédelmi e-learning tananyag keretében gondoskodik az adatvédelmi ismeretek munkavállalói képzésben felhasználható feldolgozásáról;
i) a tárgyévet követő év január 31-ig gondoskodik az elutasított tájékozódási kérelmekről szóló tájékoztatás elkészítésétől és a felügyeleti hatóság számára történő megküldéséről.

4.2.6 Adatvédelmi szakértő

Feladatai:

a) részt vesz az adatvédelmi ellenőrzések lefolytatásában;
b) az adatkezelő szervezeti egységek adatszolgáltatása alapján elvégzi az adatkezelési nyilvántartás aktualizálását;
c) vezeti az adatvédelmi incidens nyilvántartást;
d) részt vesz a Társaság adatvédelmi és adatbiztonsági szabályzatának előkészítésében és aktualizálásában;
e) ellenőrzi a számítógépeken, elektronikus adathordozókon a személyes adatok, illetve ezek felhasználásával készült dokumentumok kezelését, a dokumentumok megfelelő tárolását;
f) közreműködik az adatvédelmi tisztviselő feladatainak ellátásában;
g) részt vesz az adatvédelem terén bekövetkezett incidensek kivizsgálásában;
h) szakmai segítséget nyújt az adatkezelő szervezeti egységek részére;
i) részt vesz az adatvédelmi oktatások tematikájának kidolgozásában, a tananyagának elkészítésében, a segédletek összeállításában
j) részt vesz az Adatvédelmi Munkacsoport munkájában, a működésének megszervezésében
k) az adatvédelmi tisztviselő távolléte alatt, a kijelöléssel egyidejűleg kapott feladat-meghatározás alapján gondoskodik a 4.2.4.3 pontban felsorolt feladatok ellátásáról.

4.2.7 Adatvédelmi kapcsolattartó / területi adatvédelmi szakértő

A Társaság adatkezelési nyilvántartásába bejegyzett adatbirtokos szervezeti egység kapcsolattartója, illetve a Biztonsági főigazgatóság területi vasútbiztonsági szervezetének területi adatvédelmi szakértő feladatokkal megbízott munkavállalója. Tevékenységét érintő kérdésekben, a feladatok ellátása érdekében közvetlenül kapcsolatot tart az adatvédelmi tisztviselővel és az adatvédelmi szakértőkkel. Részt vesz az Adatvédelmi Munkacsoport munkájában.

Az adatvédelmi kapcsolattartó az adatkezelő és az adatvédelmi tisztviselő tevékenységének támogatása során

a) gondoskodik az adatkezelési nyilvántartás adatainak naprakészen tartásáról, a beállt változást azonnal közli az adatvédelmi tisztviselővel,
b) adatkezelés kapcsolattartójaként figyelemmel kíséri a szervezeti egységénél folytatott, adatkezelési nyilvántartásba vett adatkezeléseket, támogatást nyújt az adatkezelő szervezeti egység munkavállalói számára a jelen szabályzat előírásainak végrehajtásában,
c) a szervezeti egységnél bevezetésre tervezett új vagy módosítandó adatkezelési folyamat koncepció kialakítási szakaszában értesíti az adatvédelmi tisztviselőt, konzultál a megfelelő előkészítés érdekében,
d) az előírásoknak nem megfelelő adatkezelési gyakorlat észlelése esetén értesíti a szervezeti egység vezetőjét, szükség szerint előzetesen konzultál az adatvédelmi szakértővel,
e) részt vesz a területén, vagy a kijelölő szervezetén belül bekövetkezett, az adatvédelemmel összefüggő incidensek jelzésében, azok kivizsgálásában, az esemény kezelésében, szükség esetén az érintettek tájékoztatásának megszervezésében,
f) közreműködik az adatvédelmi ellenőrzési eljárás lefolytatásában,
g) a felügyeleti hatóság megkeresése esetén részt vesz a tények feltárásában, a kért információk összegyűjtésében és a választervezet elkészítésében,
h) területén közreműködik a tiszta asztal és a tiszta képernyő adatvédelmi intézkedés érvényesülése érdekében,

i) segítséget nyújt a számítógépeken, elektronikus adathordozókon a személyes adatok, illetve ezek felhasználásával készült dokumentumok megfelelő kezelési és tárolási körülményeinek kialakításában,
j) szervező munkával támogatást ad az adatvédelmi tudatosságnövelő tájékoztató előadások előkészítéséhez, illetve megtartásához.

Az előző felsorolás b)-j) pontjai esetében a területi adatvédelmi szakértő – a szervezeti feladatain túl – tevékenységét a földrajzi illetékességi területén belül más szervezetekre kiterjedően is jogosult ellátni.

4.2.8 Adatvédelmi Munkacsoport

Működtetésének célja a Társaság által kezelt, illetve feldolgozott személyes adatok kezelését végző munkaszervezetek tevékenységének összehangolása, egyúttal a Társaságon belül egységes gyakorlat kialakítása a jogszabályi előírások megfelelő alkalmazása érdekében.
A munkacsoport tevékenységét az adatvédelmi tisztviselő fogja össze, tagjai az adatvédelmi szakértők és a területi adatvédelmi szakértők.
Azon adatbirtokos munkaszervezeteknél, ahol több adatkezelés eltérő kapcsolattartóval került bejelentésre, a szervezet vezetője az adatkezelések számától, összetettségétől függően dönthet egy munkavállaló delegálásáról. Az adatvédelmi tisztviselő kezdeményezheti további munkacsoport tag kijelölését.

A munkacsoport főbb feladatai:

a) az adatkezelő szervezeti egységek és az adatkezelésekben résztvevő munkavállalók részére adandó egyeztetett tanácsok egységes értelmezések kialakítása,
b) a munkacsoport valamely tagjának kérésére megvizsgálja az adatvédelmi előírások alkalmazását érintő kérdéseket, valamint az egységes alkalmazás elősegítése érdekében legjobb gyakorlatokat dolgoz ki,
c) az adatvédelmi tudatosság szintjének növelése érdekében, a munkacsoport tagjai körében előmozdítja az adatvédelmi jogszabályokra és gyakorlatokra vonatkozó ismeretek és mintaként felhasználható dokumentációk cseréjét, szorgalmazza az adatvédelmi ismeretek eljuttatását az érintett szervezetek, személyek számára,
d) szükség szerint részleges vagy teljes (plenáris) ülést tart, amelyen a tagok az összehíváshoz igazodva személyesen vagy elektronikus úton (e-mail, audio-, vagy videokonferencia) vesznek részt,
e) a munkacsoport tagjának akadályoztatása esetén az adatkezelő szervezeti egység vezetője felelős személyesen, vagy helyettesítő kijelölése útján a folyamatos munka fenntartásáért.

4.2.9 Adatkezelést végző szervezeti egység vezetője

a) gondoskodik a feladatkörében végzett adatkezelésnek az adatkezelési nyilvántartásba történő bejelentéséről,
b) biztosítja az adatvédelmi kapcsolattartó részvételét az Adatvédelmi Munkacsoport tevékenységében; a szervezetében működő több területi adatvédelmi kapcsolattartó esetén, a munkacsoportba delegáltak számát egy főben is megállapíthatja, helyben gondoskodva arról, hogy a többi adatvédelmi kapcsolattartó is rendelkezzen a bejelentett és nyilvántartásba vett adatkezeléssel összefüggésben szükséges információkkal,
c) intézkedik az irányítása alá tartozó szervezet által kezelt személyes adatok védelméről,
d) gondoskodik az adatvédelmi szabályok végrehajtásának feltételrendszeréről,
e) intézkedik a nem szabályszerű adatkezelési gyakorlat megszüntetéséről, az eset kivizsgálása érdekében értesíti az adatvédelmi tisztviselőt és – informatikai rendszer érintettsége esetén – a rendszer üzleti tulajdonosát,
f) új adatkezelés létrehozása során irányítja a személyes adatokat tartalmazó adatbázis kialakításával összefüggő feladatok végrehajtását,
g) szervezeti egységénél irányítja és ellenőrzi a személyes adatok kezelésével, azok készítésével, továbbításával összefüggő adatvédelmi tevékenységet,
h) intézkedik az adatkezelő felé az érintett által hozzá benyújtott kérelem alapján, az érintettek jogainak (pl. hozzáférés, helyesbítés, törlés, adatkezelés korlátozása, tiltakozás, adathordozhatóság, hozzájárulás visszavonás) teljesülése érdekében.

4.2.10 Adatkezelő

Az adatkezelő feladata az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az biztosítsa az érintettek személyes adatai, személyiségi jogai védelmét. Gondoskodik az adatok kezelésének biztonságáról, megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az általános adatvédelmi rendelet, az Infotv., az IBSZ, az Iratkezelési szabályzat, valamint az egyéb adat- és titokvédelmi szabályok és az egyes rendszerek adatkezelési szabályzataiban megfogalmazottak érvényre juttatásához szükségesek. Biztosítja az érintett számára az általános adatvédelmi rendeletben meghatározott jogok érvényesülését, amelynek során elutasításra az adatvédelmi tisztviselő tudomásával és egyetértésével kerülhet sor.

Annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése az adatkezelési szabályokkal összhangban történik, adatkezelő az adatkezelés jellegére, hatókörére, körülményeire és céljaira, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével, megfelelő technikai és szervezési intézkedéseket hajt végre. Ha az adatkezelési tevékenységgel arányos, az adatkezelő adatvédelmi szabályzatban rögzíti az intézkedéseket és adatkezelési szabályokat, amelyet rendszeresen felülvizsgál és szükség szerint naprakésszé tesz.

4.2.11 Munkáltatói jogkörgyakorló

Intézkedik, hogy az általa irányított szervezeti egység munkavállalója a munkakör-, szervezetváltáskor vagy munkaviszony megszűnésekor/megszüntetésekor a munkakör átadás-átvétele során a számítógépén, a hálózati meghajtókon, pendrive-on, valamint az elektronikus postafiókjában tárolt, illetve munkakörével összefüggésben papír alapon keletkezett adatai átadása során az átadó munkavállaló személyes adatai dokumentált módon törlésre kerüljenek. Az átadott adathordozókon kizárólag az átadást követően is szükséges, a Társaság tulajdonát képező anyagok maradhatnak. Jogosult a jogkörgyakorlása körébe tartozó munkavállalók munkavállalásukkal összefüggő személyes adatait kezelni.

4.2.12 Közvetlen munkahelyi vezető

Ellátja a személyes adatok kezelése során azokat a feladatokat, amelyek nem tartoznak a munkáltatói jogkörgyakorló kizárólagos jogkörébe, vagy amelyeket a munkáltatói jogkörgyakorló számára delegál.

4.2.13 Személyes adatokat kezelő munkavállaló

A Társaság személyes adatokat kezelő munkavállalója

a) kezeli és megőrzi a feladata, illetve a munkaköre ellátása során birtokába került adatokat;
b) maradéktalanul érvényesíti az adatvédelmi előírásokat az adatkezelés teljes folyamatában;
c) betartja az adatkezelésre vonatkozó előírásokat;
d) ügyel a nyilvántartások biztonságos kezelésére és tárolására;
e) gondoskodik arról, hogy az általa kezelt adatokhoz illetéktelen személy ne férhessen hozzá;
f) szükség szerint feltünteti a személyes adatot tartalmazó adathordozókon és dokumentumokon a „*Zártan kezelendő!*” kezelési jelölést;
g) indokolt esetben törli a személyes adatokat, illetve – a tárolás kivételével – korlátozza az adatokhoz történő hozzáférést;
h) gondoskodik arról, hogy az informatikai eszközök adathordozóján tárolt személyes adatok törlése esetén azok a későbbiekben ne legyenek visszaállíthatók;
i) a Társasághoz belépéskor, és azt követően rendszeresen részt vesz a Társaságnál szervezett információ- és adatvédelmi oktatásokon, illetve elvégzi e témakörben számára előírt e-learning kurzusokat;
j) feladatellátása során haladéktalanul megszünteti az adatkezeléssel kapcsolatban feltárt visszásságot, az adatvédelmi tisztviselővel egyeztetve.

4.2.14 Adatvédelmi tisztviselők egyeztető fóruma

A MÁV-csoport tagvállalatainál kijelölt adatvédelmi tisztviselők, illetve – ennek hiányában – adatvédelmi felelős munkavállalók szakmai fóruma, amely lehetőséget biztosít a MÁV-csoport

szintjén felmerülő adatkezelési feladatok szakmai egyeztetésére. Összehívását a MÁV Zrt. adatvédelmi tisztviselője kezdeményezi.

Az Adatvédelmi tisztviselők egyeztető fóruma működtetésének főbb szempontjai:

a) működtetésének célja, hogy a rendszeresen, illetve időszakosan összehívott egyeztetések alkalmával az egyes társaságokon átívelő, több társaságot, illetve a MÁV-csoport egészét átfogóan érintő adatkezelések tekintetében, illetve több társaság által igénybe vett azonos adatfeldolgozó irányában az egységes gyakorlat kialakítása,
b) az MÁV-csoport tagvállalatai körében előmozdítja az adatvédelmi jogszabályokra és gyakorlatokra vonatkozó ismeretek és mintaként felhasználható dokumentációk megosztását,
c) az érintettek irányában az adatkezelések áttekinthetősége érdekében a tájékoztatás szerkezetének, tartalmának az érintetti jogok gyakorlásának összehangolt csatornákon és módokon történő eljuttatása,
d) az adatkezelési nyilvántartásokban szereplő adatkezelések főbb mutatóinak időszakos egyeztetése az esetleges azonos jellegű vagy közös adatkezelések feltárása és a nyilvántartások ezirányú aktualizálása érdekében,
e) az adatfeldolgozóra mutató nyilvántartásban szereplő adatkezelések összehangolt szerepeltetése az adatkezelői és az adatfeldolgozói szerepet betöltő társaságok nyilvántartásaiban,
f) a MÁV-csoport egészét vagy több tagvállalatát érintő adatvédelmi incidens esetén a fórum tagjai egyeztetik az incidens kivizsgálásának főbb lépéseit, különösen a közös adatkezelések, vagy közösen igénybe vett adatfeldolgozó vonatkozásában,
g) a NAIH több tagvállalatot érintő megkeresése esetén a fórum érintett tagjai feladatmegosztással részt vesznek a tények kiderítésében, a szükséges információk összegyűjtésében, a dokumentumok egyeztetett, egymásnak nem ellentmondó létrehozásában, a kívánt adatok kitöltésében és a választervezet elkészítésében,
h) az adatvédelmi tisztviselők által képviselt társaságok által kezelt, illetve feldolgozott személyes adatokkal összefüggően, a szervezetek tevékenységének bemutatása a MÁV-csoport egyéb tagvállalatai számra, az egységes gyakorlat kialakítása a jogszabályi előírásoknak összehangolt megfelelés érdekében.

4.2.15 Üzleti tulajdonos

az általa tulajdonolt informatikai rendszer vonatkozásában

a) gondoskodik az adatvédelmi szabályok érvényre juttatásáról, a rendszerben található személyes adatok védelméről,
b) nem szabályszerű adatkezelési gyakorlat esetén intézkedik annak megszüntetéséről,
c) irányítja és ellenőrzi a személyes adatok kezelésével, azok készítésével, továbbításával összefüggő adatvédelmi tevékenységet.

4.2.16 Jogi főigazgatóság

Jogi szakvéleményével támogatja az adatkezelőt vagy adatfeldolgozót a jogszabályi előírások teljesítésében, valamint a felügyeleti hatóságnak a Társaságot érintő intézkedése esetén. A Társaság belső szabályozási tevékenységének, normarendszerének felügyelete és koordinálása, a jogszabályi megfelelőség és a szabályzatok összhangjának biztosítása keretében vizsgálja, hogy a szabályzatok készítéséért felelős szervezetek biztosítottak-e az adatvédelmi tisztviselő számára véleményezési lehetőséget azon normatív utasítások készítése, módosítása folyamatában, amelyek olyan adatkezelésre vonatkoznak, ahol a személyes adatok kezelését is érintő adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

a) Ezek az általános adatvédelmi rendelet 35. cikkének (1), illetve (3) bekezdésében megjelölt adatkezelések:
   - valószínűsíthetően magas kockázattal járó, különösen új technológiákat alkalmazó adatkezelés,
   - a személyes jellemzők automatizált adatkezelésen alapuló módszeres és kiterjedt értékelése, amelyre a természetes személyt jelentős mértékben érintő döntések épülnek;
   - nagyszámú különleges személyes adat kezelése;
   - közforgalom számára nyilvános helyek nagymértékű, módszeres megfigyelése.

b) Ezeken túl a NAIH által kiadott és a honlapján (www.naih.hu) közzétett azon jegyzékben felsoroltak, amely esetekben adatkezelésre vonatkozóan a hatásvizsgálat elvégzése kötelező (pl. a helymeghatározási adatok kezelése, ha az módszeres megfigyelésre vagy profilalkotásra utal, illetve a munkavállaló munkájának megfigyelése).

A véleményezési lehetőség hiányának megállapítása esetén a szabályzatmenedzsment folyamatot visszairányítva felhívja az adott szabályzat készítéséért felelős szervezetet az adatvédelmi tisztviselővel történő kötelező egyeztetés lefolytatására.

A személyes adatok védelméhez kapcsolódóan, az adatvédelmi tisztviselő megkeresésére állásfoglalást ad a Társaság működésével, a pályahálózat üzemeltetésével összefüggően alkalmazandó jogszabályok értelmezése tekintetében.

Állásfoglalást ad az érintett vagy egy másik természetes személy létfontosságú érdekei védelme érdekében történő adatkezeléssel összefüggésben a jogi cselekvőképtelenségre vonatkozóan.

4.2.17 Adatfeldolgozó

Adatkezelő, ha nevében az adatkezelést más végzi, az kizárólag olyan adatfeldolgozót vehet igénybe, aki vagy amely megfelelő garanciákat nyújt az adatkezelés követelményeinek való megfelelésére és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. Az adatfeldolgozó személyéről az érintetteket előzetesen tájékoztatni szükséges.

A Társaság által megbízott adatfeldolgozó személyes adatok kezelésével kapcsolatos feladatait – az adatkezelésre vonatkozó jogszabályi előírások keretei között – a Társaság határozza meg.

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

Az adatfeldolgozó tevékenységének ellátása során további adatfeldolgozót a Társaság rendelkezései alapján vehet igénybe. Amennyiben az adatfeldolgozó további adatfeldolgozót kíván megbízni egyes adatkezelési műveletek elvégzésével, ehhez a Társaság előzetes írásbeli hozzájárulására van szükség. Az adatkezelésben érintettek vonatkozásában olyan szerződéses kötelezettségeket kell meghatározni, amely az adatkezelés teljes folyamatában biztosítja a megfelelő védelmi szintet.

Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben.

A Társaságnak az adatfeldolgozóval kötött szerződést, illetve megállapodást írásba kell foglalnia. Az iratnak minden olyan információt tartalmaznia kell, amely a személyes adatok kezelése szempontjából releváns. Az adatfeldolgozói megállapodásra vonatkozó előírásokat a 7.6 számú melléklet tartalmazza. Adatfeldolgozóként nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben akár közvetett, akár közvetlen módon érdekelt. A feltételek kidolgozása során biztosítani szükséges az adatvédelmi tisztviselő véleményezési lehetőségét.

4.2.18 Közös adatkezelés

Amikor az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg, azok közös adatkezelőknek minősülnek. Amennyiben jogszabály nem határozza meg, a közös adatkezelőknek átlátható módon, a közöttük létrejött megállapodásban kell meghatározniuk a kötelezettségek teljesítéséért fennálló – különösen az érintett jogainak gyakorlásával és az információk rendelkezésre bocsátásával kapcsolatos – feladataikkal összefüggő felelősségük megoszlását.

a) a közös adatkezelésben résztvevő adatkezelők közötti viszonyrendszert rögzítő megállapodás célja, hogy a többes adatkezelési szituációkban is egyértelmű legyen a jogosultságok kezelésének rendszere, az adatvédelmi szabályok betartásáért, illetve esetleges megszegéséért való felelősség, ezáltal a többes adatkezelés során se csökkenjen a személyes adatok védelme,

b) meg kell határozni a feladatokkal összefüggő kötelezettségek adatkezelők közötti megoszlását, mivel a közös adatkezelésben befolyással rendelkezés nem jelent egyúttal azonos mértékű végrehajtási felelősség meglétét is, ezért a felek egyes adatkezelési mozzanatoknál fennálló felelősségét a megállapodásban külön kell rögzíteni,

c) a megállapodásnak tükröznie kell a közös adatkezelők érintettekkel szembeni szerepét és a velük való kapcsolatukat; az érintettek irányába az adatkezelés okozta károkért a közös adatkezelésben résztvevők egyetemleges felelőssége mellett az adatkezelők a különböző szakaszokban eltérő mértékben lehetnek felelősek a személyes adatok kezeléséért, ezáltal a kárfelelősség mértékének sem szükséges megegyezőnek lennie, amelyet a megállapodásnak tartalmaznia kell,

d) különös figyelemmel kell lenni az érintettek jogainak gyakorlásával és számukra az információk rendelkezésre bocsátásával kapcsolatos teendőkre, azaz ki teljesíti az érintettek jogait és ki adja meg számukra az adatkezelési tájékoztatást,

e) rögzíteni szükséges egy adatvédelmi incidens bekövetkezésének esetére a belső feladatmegosztást,

f) kapcsolattartót lehet kijelölni a megállapodásban az érintettek számára,

g) a közös adatkezelésre vonatkozó megállapodás lényegét az érintettek rendelkezésére kell bocsátani,

h) az érintettek részére átadott tájékoztatóban szerepeltetni szükséges azt is, hogy az érintett a megállapodásban rögzített feltételektől függetlenül mindegyik adatkezelő vonatkozásában és mindegyik adatkezelővel szemben gyakorolhatja a jogait.

A közös adatkezelői státus további szempontjai:

a) Ha a cél elérése a közös adatkezelésben résztvevő másik adatkezelő nélkül nem lehetséges, a közös adatkezelés fennáll.

b) Közös adatkezelés megállapíthatósága valószínű az egységes célok mentén, azonos informatikai rendszer vagy platform használata, egyazon adatbázisba a tevékenységek összehangolásával történő adatgyűjtés (pl. egységes ügyfélkezelő rendszer) esetén.

c) Nem feltétel az, hogy a közös adatkezelésben résztvevő adatkezelők mindegyike meghatározó módon, azonos mértékben működjön közre az adatkezelésben.

d) Nem szükséges mindegyik adatkezelőnek átfognia az adatkezelés minden lépését.

e) A személyes adatokhoz való hozzáférés, a személyes adatok fizikai birtoklása nem feltétele a közös adatkezelői minőségnek, ezért nem akadályozza a közös adatkezelés megállapítását amennyiben a közös adatkezelők valamelyike nincs az adatok birtokában és nem fér hozzá az adatokhoz, ha egyébként az adatkezelés céljának és/vagy eszközeinek meghatározásában valamely részt vállalnak.

f) A közös adatkezelők egymás között külön-külön is címzetteknek minősülnek és önálló jogalappal kell rendelkezniük a személyes adatok egymás közötti továbbításához.

g) A hozzájáruláson alapuló adatkezelés esetén a hozzájárulásnak a közös adatkezelők közötti adattovábbítást is át kell fognia.

h) Új közös adatkezelő csak akkor léphet be a folyamatban levő adatkezelésbe, ha erre maga is megfelelő jogalappal rendelkezik és erről az érintetteknek megfelelő tájékoztatást kapnak.

i) A közös adatkezelői megállapodás elmaradása esetén is, a tényleges tevékenység alapján egyetemlegesen felelnek a felek.

j) Mivel a közös adatkezelési szituációk magasabb kockázatot jelenthetnek az érintett jogaira és szabadságaira, ennél fogva vizsgálandó, hogy szükséges-e adatvédelmi hatásvizsgálatot lefolytatni.

A közös adatkezelést körültekintően kell elhatárolni az adatfeldolgozói kapcsolattól, mert nem adatfeldolgozói kapcsolat az, ha az adatfeldolgozónak lehetősége van az adatkezelés céljainak és lényeges eszközeinek meghatározásában (pl. egy kiszervezési kapcsolat a közös adatkezelés hatálya alá tartozik, ha megállapíthatóak a közös célok és a lényeges eszközökről való döntés egyaránt).

4.3 Az érintettek jogai és érvényesítésük

Az adatkezelőnek megfelelő intézkedéseket kell hoznia annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. Az adatkezelésben érintettnek a személyes adatai kezelésével összefüggésben – az alkalmazott jogalaptól függően – az alábbi jogai vannak, illetve lehetnek.

jogalap / érintetti jog	hozzájárulás	kifejezett hozzájárulás	szerződés teljesítése	jogi kötelezettség teljesítése	létfontosságú érdek védelme	közérdekű feladat végrehajtása	jogos érdek	jogi igények előterjesztése, érvényesítése, illetve védelme
átlátható tájékoztatás	+	+	+	+	+	+	+	+
hozzáférés	+	+	+	+	+	+	+	+
helyesbítés	+	+	+	+	+	+	+	+
törlés	+	+	+	-	+	-	+	-
elfeledtetés	+	+	+	-	+	-	+	-
adatkezelés korlátozása	+	+	+	+	+	+	+	+
adathordozhatóság (elektronikus feldolgozás)	+	+	+	-	-	-	-	-
tiltakozás	-	-	-	-	-	+	+	-
tiltakozás az automatizált döntéshozatal ellen	+	-	-	-	+	+	+	+
hozzájárulás visszavonása	+	+	-	-	-	-	-	-

4.3.1 A tájékoztatáshoz való jog

A tájékozódáshoz való jog értelmében az adatkezelőnek megfelelő intézkedésekkel biztosítania kell az érintett részére, hogy a személyes adatok kezelésére vonatkozó valamennyi információt tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtson az érintett személyes adatai kezelésének útjával és körülményeivel kapcsolatban. Ezen jog egyrészről azt hivatott tudatosítani az adatalanyokban, hogy az adatkezelő velük kapcsolatban személyes adatokat kíván kezelni, másrészről a tájékoztatás révén az adatalanyok megítélhetik, hogy a magánéletükre milyen hatást gyakorolhat a tervezett adatkezelés, illetve milyen egyéb kockázatokat és veszélyeket rejt magában. Az érintettek a kapott információk alapján gyakorolhatják az információs önrendelkezési jogukat is.

Rendelkezésre bocsátandó információk a tájékoztatáshoz, illetve a hozzáféréshez való jog esetén:

információ	az érintett joga	
	tájékoztatáshoz	hozzáféréshez
az érintettre vonatkozó személyes adatkezelés ténye	–	+
az adatkezelő és képviselőjének adatai	+	–
az adatvédelmi tisztviselő elérhetőségei	+	–
az adatkezelés célja	+	+
az adatkezelés jogalapja	+	+
az adatkezelő vagy harmadik fél jogos érdekei (jogos érdeken alapuló adatkezelés esetén)	+	+
személyes adatok kategóriái (amennyiben azokat nem az érintettől gyűjtik)	+	+
személyes adatok címzettjei vagy a címzettek kategóriái	+	+
külföldre történő adattovábbítás	+	+
A személyes adatok megőrzési ideje, vagy a megőrzési idő meghatározásának szempontjai	+	+
érintetti jogok (hozzáférés, helyesbítés, törlés, kezelés korlátozása, tiltakozás, adathordozhatóság, hozzájárulás visszavonás)	+	+
jogorvoslati lehetőségek (felügyeleti hatóság, bíróság)	+	+
profilalkotás alkalmazásának esetén annak ténye	+	+
a felmerült adatvédelmi incidensek körülményei	–	+
automatizált döntéshozatal (ténye, alkalmazott logika, a döntéshozatal eredményét alátámasztó megfontolások, tényezők)	+	+
adatbiztonsági intézkedések	+	+
ha az adatok megadása törvény vagy szerződés alapján kötelező	+	+
az adatok forrása (amennyiben azokat nem az érintettől gyűjtik)	+	+
az adatkezelés tárgyát képező személyes adatok másolata	–	+

Ha a személyes adatok nem az érintettől származnak, csak abban az esetben mellőzhető az információnak az érintett számára történő biztosítása ha:

- az érintett már rendelkezik az információval;
- az érintett tájékoztatása lehetetlen vagy aránytalan erőfeszítést jelentene;
- az lehetetlenné tenné vagy súlyosan rontaná a az adatkezelés célkitűzéseinek elérését;
- ha a kezelt személyes adatok gyűjtését, továbbítását vagy közzétételét az adatkezelőre vonatkozó törvény kifejezetten előírja;
- a személyes adatok kezelésre vonatkozó törvény titoktartási kötelezettséget ír elő.

4.3.2 A helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését. Az adatkezelő a hibás személyes adatot, amennyiben a valóságnak megfelelő személyes adat a rendelkezésére áll, saját kezdeményezésre, illetve az érintett kérésére, az általa bemutatott dokumentumok alapján helyesbíti, illetve az adatfeldolgozónál helyesbítteti. Az adatkezelőnek meg kell jelölnie az általa kezelt személyes adatot, ha az érintett annak helyességét vagy pontosságát vitatja, de a rendelkezésre álló dokumentumok alapján nem állapítható meg egyértelműen annak helytelensége vagy pontatlansága.

4.3.3 A törléshez való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje meghatározott feltételek esetén.

Az érintett személyes adatait törölni kell, ha:
- a személyes adatok kezelésének célja megszűnt;
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen;
- az adatkezelés jogellenes;
- a törlést uniós vagy tagállami jog előírja, vagy a felügyeleti hatóság elrendelte;
- a személyes adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

A törlést nem kell alkalmazni, amennyiben az adatkezelés szükséges – többek között – a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből, illetve az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából, vagy amennyiben az adatra jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez van szükség.

Törlés helyett az adatkezelő – az érintett kérelmére, vagy ha a rendelkezésre álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit – korlátozza személyes adatai kezelését. A korlátozott személyes adat kizárólag azon adatkezelési cél fennállásáig kezelhető, amely kizárta a személyes adat törlését.

4.3.4 Az elfeledtetéshez való jog

Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, és az elérhető technológia és a megvalósítás költségeinek figyelembevételével meg kell tennie az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket is – annak érdekében, hogy tájékoztassa az adatkezelő szervezeti egységet, hogy az érintett kérelmezte tőle a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

4.3.5 Az adatkezelés korlátozásához való jog

Az érintett kérésére az adatkezelőnek korlátoznia kell az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;

b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;

d) az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A korlátozás alá eső személyes adatokat – a tárolás kivételével – csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni. Az adatkezelés korlátozásának feloldásáról adatkezelőnek előzetesen tájékoztatnia kell azt az érintettet, akinek a kérésére korlátozta az adatkezelést.

4.3.6 Az adathordozhatósághoz való jog

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja ha

a) az adatkezelés hozzájáruláson, vagy szerződésen alapul és
b) az adatok feldolgozása elektronikusan történik.

Jogosult továbbá arra, hogy az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, vagy kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

4.3.7 A tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a kezelése ellen, ha a személyes adatok kezelésére az adatkezelő jogos érdeke, vagy közérdekű, illetve közhatalmi jellege miatt kerül sor. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy olyan kényszerítő erejű jogos okok indokolják az adatkezelést, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

4.3.8 Tiltakozás közvetlen üzletszerzés estén

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

4.3.9 Tiltakozás az automatizált döntéshozatal ellen

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

4.3.10 Az érintett hozzáféréshez fűződő joga

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és az általános adatvédelmi rendeletben felsorolt információkhoz hozzáférést kapjon. Az előzetes tájékoztatással ellentétben a hozzáférés alapján – főszabály szerint – az érintett döntésétől függ az, hogy benyújt-e e jog érvényesítésére vonatkozó kérelmet vagy sem.

Az érintett jogosult arra, hogy hozzáférést kapjon a személyes adataihoz és tájékoztatást kapjon az alábbi információkhoz:

a) a kezelt személyes adatok forrása,
b) az adatkezelés célja és jogalapja,
c) a kezelt személyes adatok köre,
d) a kezelt személyes adatok továbbítása esetén az adattovábbítás címzettjeinek – ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket – köre,
e) a kezelt személyes adatok megőrzésének időtartama, ezen időtartam meghatározásának szempontjai,
f) az érintettet megillető jogok, valamint azok érvényesítése módjának ismertetése,
g) profilalkotás alkalmazásának esetén annak ténye és az érintett személyes adatainak kezelésével összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményei, azok hatásai és az azok kezelésére tett intézkedések.

A Társaság biztosítja azt, hogy az érintettek tájékozódhassanak az őket érintő adatkezelésekről, illetve a róluk kezelt adatokat megismerhessék és a kezelt adatokat tartalmazó iratokról másolatot vagy kivonatot kaphassanak (az adatigénylő lap a 7.10 számú mellékletben található). Az érintett erre vonatkozó igényét az adatkezelőnél, vagy közvetlenül az adatvédelmi tisztviselőnél nyújthatja be.

Amennyiben érintett ettől eltérő címzett számára küldi meg az igénylését, a címezettnek haladéktalanul gondoskodnia kell az igény továbbításáról az adatkezelő szervezeti egységhez.

Az adatkezelés tárgyát képező személyes adatok másolatát díjmentesen kell az érintett rendelkezésére bocsátani. Az érintett által kért további másolatokért az adminisztratív költségeken alapuló, észszerű mértékű díj számítható fel. Az adatkezelő megtagadhatja a hozzáférés iránti kérelem teljesítését, amennyiben az adatalany kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó.

A másolat kiadásához való jog biztosítja az érintett számára a személyes adataihoz való tényleges hozzáférését. A másolathoz való jog speciális esete a kamerafelvételek kiadása. Egyes törvények rendelkezéseihez képest az általános adatvédelmi rendelet értelmében az érintettnek nem kell igazolnia a másolat kiadásához való jogos érdekét, illetve nem kell indokolnia, hogy mi okból kíván élni a személyes adataihoz hozzáférés jogával. A másolat kiadásához fűződő jog gyakorlása azonban nem érintheti hátrányosan mások jogait és szabadságait, ebből kifolyólag az érintett másolathoz való joga alapján továbbra sem kaphatja meg a kamerafelvétel olyan másolatát, amelyen más érintett képmása és cselekvése kitakarás nélkül szerepel. Az adatkezelő ilyen esetben köteles a kitakarás elvégzésére, kivéve, ha az érintett hozzájárul a képmásának és cselekvésének kitakarás nélküli kiadáshoz.

Adatkezelő indokolatlan késedelem nélkül, de a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet.

A kérelem elutasítása esetén az adatkezelő a kérelem kézhezvételét követő egy hónapon belül írásban közli az elutasítás indokait, továbbá tájékoztatja az érintettet a bírósági jogorvoslat, valamint a felügyeleti hatósághoz fordulás lehetőségéről.

4.4 Az adatvédelmi szabályok megtartásának ellenőrzése

Az adatvédelmi és adatbiztonsági intézkedések betartásának, valamint jelen szabályzat rendelkezései érvényesülésének ellenőrzésére jogosultak:

a) a Társaság elnök-vezérigazgatója,
b) az adatvédelmi tisztviselő,
c) az Információ- és adatvédelem szervezet vezetője,
d) az adatvédelmi szakértő,
e) a területi adatvédelmi szakértő,
f) a Társaság elnök-vezérigazgatója egyedi döntésével kijelölt személy (pl.: belső ellenőr),
g) jogszabályban erre felhatalmazott személy (például a NAIH tisztviselői),
h) a Társaság által megbízott tanúsító szervezet.

Az ellenőrzésnek különösen az alábbiakra kell kiterjednie:

a) adatkezelési tájékoztató (pl. piktogramok), adatvédelmi nyilatkozat, adatkezelési hozzájárulás,
b) helyi adatkezelési szabályzat,
c) adatkezelési nyilvántartásba bejelentés,
d) érdekmérlegelési teszt,
e) betekintési- és hozzáférési jogosultság naprakészsége,
f) fizikai biztonsági (pl. IBSZ előírásaiból eredő adatbiztonsági) előírások érvényesülése,
g) jelszóházirend, jelszavak időszakonkénti cseréje,
h) adathordozók kezelésének szabályozottsága, nyilvántartása, megléte,
i) iratkezelési szabályok betartása, selejtezés, megsemmisítés végrehajtása, dokumentálása,
j) általános adatvédelmi rendelet, Infotv. és további adatvédelmi előírásokat tartalmazó jogszabályok, valamint a jelen szabályzat rendelkezéseinek betartása.

4.4.1 Adatvédelmi ellenőrzési eljárás

Az adatvédelmi ellenőrzési eljárás célja, hogy az adatvédelmi tisztviselő – szükség szerint az adatvédelmi kapcsolattartó valamint a területi adatvédelmi szakértők bevonásával – meggyőződjön arról, hogy a Társaság az adatvédelemmel kapcsolatos jogszabályoknak és belső szabályzatoknak megfelelően kezeli-e a személyes adatokat.

Az adatvédelmi tisztviselő átfogó ellenőrzés esetén megtervezi az adatkezelés ellenőrzési feladatait, amely alapján az ellenőrzés lefolytatásáról tájékoztatja az érintett szervezeti egység vezetőjét, elegendő időt biztosítva a felkészüléshez. A szervezeti egység vezetője köteles gondoskodni arról, hogy az adatvédelmi tisztviselő lefolytathassa az ellenőrzését, illetve kellően megindokolt esetben – legfeljebb három munkanapon belül – új időpontra tehet javaslatot.

Az adatvédelmi tisztviselő ellenőrzése során az érintett szervezeti egység irodahelyiségeibe beléphet, irataiba, elektronikus dokumentumaiba betekinthet, munkatársaitól tájékoztatást kérhet a konkrét adatkezeléssel összefüggésben.

Az adatvédelmi tisztviselő az ellenőrzését az általános adatvédelmi rendelet elszámoltathatóság elvének megfelelően dokumentálja (ellenőrzött szervezeti egység, illetve adatkezelés, időpontja, időtartama, a vizsgált körülmények, adatok, megállapítások stb.).

Amennyiben az adatvédelmi tisztviselő megállapítja, hogy az adatkezelés az ellenőrzés alá vont szervezeti egységnél nem a jogszabályoknak, illetve a belső szabályzatoknak megfelelően történik, javaslatot tesz a szabályszerű adatkezelés – meghatározott határidőn belül történő – helyreállítására. Az ezek alapján megtett intézkedésekről a szervezeti egység vezetője a kijelölt határidőn belül tájékoztatást nyújt. Az adatvédelmi tisztviselő az intézkedéseket, illetve azok betartását utóellenőrzés keretében jogosult ellenőrizni.

Az adatkezelést végző szervezeti egység vezetője felkérésének eleget téve is végezhet ellenőrzést az adatvédelmi tisztviselő.

Az adatvédelmi tisztviselő jogellenesség megállapítása hiányában is adhat tájékoztatást az adatkezelő számára a szervezeten belüli és kívüli, általa legjobb gyakorlatnak ítélt eljárásokról, valamint a jövőre nézve javasolni megfelelőbb eljárás vagy eljárások alkalmazását. Az adatvédelmi tisztviselő ezen javaslatok követésére is kitérhet a soron következő vizsgálata során.

4.4.2 Adatvédelmi audit

Az adatvédelmi audit célja a végzett vagy tervezett adatkezelési műveletek adatvédelmi szempontok alapján történő értékelésén keresztül, a magas szintű adatvédelem és adatbiztonság megvalósítása és a jogszerű adatkezelés biztosítása. Tervezett adatkezelési műveletek akkor vonhatók előzetes audit alá, ha az adatkezelésre vonatkozó koncepció kidolgozottsága ezt lehetővé teszi. Az adatvédelmi auditot az adatvédelmi tisztviselő az adatkezelő kérésére, illetve indokolt esetben (magas maradó kockázatú adatkezelés esetén) saját döntése alapján folytatja le, amelybe informatikai, illetve távközlési rendszerek érintettsége esetén bevonhatja az Informatikai és technológiai rendszerek főigazgatóság illetékes szakmai egységét, esetleg külső adatvédelmi szakértő bevonását kezdeményezi.

Az auditor az adatvédelmi audit eredményét az erről készített értékelésben foglalja össze, amelyben javaslatokat fogalmazhat meg az adatkezelő számára. Az adatvédelmi audit az adatvédelmi tisztviselő e szabályzatban rögzített egyéb hatásköreinek gyakorlását nem korlátozza.

4.4.3 Közreműködés a felügyeleti hatóság vizsgálatában

A Társaságnál a felügyeleti hatóság jogosult az adatvédelmi szabályok megtartását ellenőrizni, illetve kivizsgálni a hozzá érkező bejelentésekben foglaltakat. A felügyeleti hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy a személyes adatok kezelésével kapcsolatban a Társaságnál jogsérelem következett be, vagy annak közvetlen veszélye fennáll.

Az adatvédelmi tisztviselő szakvéleményével támogatja az adatkezelőt vagy adatfeldolgozót a felügyeleti hatóságnak a Társaságot érintő intézkedése esetén. Szükség esetén – az adatkezelést végző

szervezeti egység vezetője, illetve a Jogi főigazgatóság bevonásával – együttműködik a felügyeleti hatósággal, kérésüknek az általuk megállapított határidőn belül eleget tesz. Amennyiben a felügyeleti hatóság által tett megállapításokkal, illetve az általuk meghozott határozatokkal nem ért egyet, a Jogi főigazgatóság szakvéleményét beszerezve, a Társaság elnök-vezérigazgatója útján megteszi az általános adatvédelmi rendeletben meghatározott lépéseket. A felügyeleti hatóság Társaságot érintő intézkedése esetén az adatvédelmi tisztviselő együttműködik az adatkezelővel, illetve az adatfeldolgozóval a jogszabályi előírások teljesítése érdekében.

4.4.4 Az adatvédelmi rendelkezések megsértése észlelése esetén a munkavállalók által követendő eljárás

Az adatvédelmi szabályok megsértése, vagy ennek közvetlen veszélye észlelése esetén, bárki közvetlenül az adatvédelmi tisztviselőhöz fordulhat. Az adatvédelmi tisztviselő a bejelentés megalapozottsága, illetve az adatvédelmi előírások megsértésének észlelése esetén annak megszüntetésére szólítja fel az adatkezelőt. Azokkal a munkavállalókkal szemben, akik a Társaság adatvédelmi és adatbiztonsági szabályzata előírásait megsértették, az érintett munkáltatói jogkörgyakorlójánál hátrányos jogkövetkezmény megállapítására vonatkozó munkáltatói intézkedést, esetlegesen tényfeltáró vizsgálatot kezdeményez. A megállapítás, illetve a tényfeltáró vizsgálat az adatvédelmi tisztviselő bevonásával történik.

A tényfeltáró vizsgálat lefolytatására, a vétkes kötelezettségszegés megállapítására, a hátrányos jogkövetkezmények és más munkajogi intézkedések alkalmazására a munkaviszonyra vonatkozó szabályok (KSZ, belső szabályzatok, utasítások) irányadóak. A szankcióknak arányban kell állniuk a kötelezettségszegés súlyával és az okozott kárral.

4.5 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, amely megfelelő és kellő idejű intézkedés hiányában a természetes személyek számára fizikai, vagyoni vagy nem vagyoni károkat okozhat.

Adatvédelmi incidens lehet többek között:

- a személyes adatok feletti rendelkezés elvesztése (pl. pendrive, notebook elvesztése, személyes adatokat tartalmazó e-mail üzenet helytelen címre történő elküldése),
- a személyazonosság-lopás vagy a személyazonossággal való visszaélés,
- az álnevesítés engedély nélküli feloldása,
- személyes adatokat tartalmazó adatbázis sérülése,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése.

Érzékeny adatok lehetnek különösen:

- különleges személyes adatok (pl. érdekképviseleti tagság),
- személyiség lopásra alkalmas adatok,
- felhasználónevek és jelszavak,
- az érintett pénzügyi helyzetére vonatkozó, társadalmi megbecsülésére kiható adatok.

Adatvédelmi incidens bekövetkezéséről haladéktalanul tájékoztatni kell az Információ- és adatvédelem szervezet vezetőjét, illetve a Társaság adatvédelmi tisztviselőjét a közzétett elektronikus vagy telefonos elérhetőségén.

Adatvédelmi incidensre utaló információ esetén azt kell először megvizsgálni, 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. Amennyiben nem állapítható meg incidens megtörténte, akkor azt kell vizsgálni, hogy e szabályzat helyett az IBSZ-t, a Vagyonvédelmi utasítást, vagy bármely más belső szabályzatot, esetleg egyéb jogszabályt sért-e. Amennyiben egyértelmű az

incidens megtörténte, akkor a következő bekezdések végrehajtásával szükséges további lépéseket megtenni.

Adatvédelmi incidens bekövetkezése esetén kockázatértékelést kell végrehajtani, amelynek során az alábbi szempontokat kell figyelembe venni, amelyekre a bejelentésben ki kell térni:

- az incidens bekövetkezésének időpontja,
- az incidens jellege,
- a személyes adatok típusa és mennyisége,
- az érintettek száma,
- az incidens lehetséges következményei az érintettek számára,
- az érintettek azonosíthatóságának egyszerűsége.

Amennyiben az adatvédelmi tisztviselőnek olyan incidens jut tudomására, amely valószínűsíthető kockázattal jár a természetes személyek jogaira és szabadságaira nézve, arról indokolatlan késedelem nélkül, de legkésőbb 72 órán belül tájékoztatja a felügyeleti hatóságot, illetve ha az incidens magas kockázattal jár, gondoskodik az érintettek tájékoztatásáról is. Az tájékoztatásnak tartalmaznia kell az adatvédelmi incidens jellegének leírását, valamint az érintetteknek szóló, a lehetséges hátrányos hatások enyhítését célzó ajánlásokat. A tájékoztatásról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és az általa vagy más érintett hatóságok által adott útmutatások tiszteletben tartásával. A tájékoztatás csak kivételes körülmények között maradhat el.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat 5 évig meg kell őrizni.

4.6 Az adatvédelmi incidensek megelőzése, felderítése, kezelése

Az adatkezelő szervezeti egységeknek már az adatkezelés kialakítása során törekedniük kell arra, hogy az adatvédelmi incidenseket kellő időben felismerjék. Ennek érdekében, monitorozniuk szükséges az adatkezelésüket, valamint fel kell készülniük egy esetleges incidens bekövetkezése esetén annak hatásainak behatárolására, felmérésére, az érintettek tájékoztatására, mind a csatorna előzetes megtervezésével (e-mail, honlap stb.), mind pedig az incidens lehetséges főbb esetei vonatkozásában kiküldendő kommunikáció tartalmára vonatkozóan, ami adott estben több lépcsős is lehet.

Az incidensek megelőzése, felderítése és megfelelő kezelése érdekében az adatkezelés megkezdése előtt incidenskezelési szabályozást kell készíteni, amelyben legalább az alábbiakra ki kell térni:

- a döntéshozatali eljárásrend meghatározása;
- a jelentési eljárásrend meghatározása, jelentési kötelezettség előírása;
- az incidens kezelési feladatok meghatározása;
- az adatvédelmi tisztviselő bevonásának esetkörei és szabályai;
- szakértő bevonásának esetkörei és szabályai;
- az incidens nyilvántartás szabályai;
- a kommunikációs levélminták elkészítése;
- az incidens észlelés eszközrendszerének meghatározása;
- a felelősségek meghatározása.

4.7 Nyilvántartások

4.7.1 Adatkezelési nyilvántartás

Az adatkezelést végző szervezeti egység vezetője nyilvántartásba vétel céljából, a 7.5 számú melléklet alapján köteles a Társaság adatvédelmi tisztviselőjének bejelenteni az adatkezelésre vonatkozó adatokat, egyúttal adatvédelmi kapcsolattartót jelöl ki, továbbá az adatkezelésre vonatkozóan helyi adatvédelmi és adatkezelési szabályozást ad ki, amely az adatkezelésre vonatkozó bejelentésben szereplő adatokon túlmenően tartalmazza az adatokhoz hozzáféréssel rendelkezők körét, jogosultságát, a kezelt személyes adatoknak a főbb munkafolyamatokhoz való kapcsolódását, valamint az adatok elektronikus feldolgozása esetén az adatok mentésének, azok tárolásának rendjét és az adatok feldolgozására, esetlegesen közös feldolgozására vonatkozó megállapodást is. Az adatkezelésről szóló bejelentést, valamint a helyi adatvédelmi és adatkezelési szabályozást az adatkezelés megkezdését megelőzően legalább 5 munkanappal korábban kell megküldeni az

adatvédelmi tisztviselő számára a nyilvántartás napra készen történő tartása céljából. Meglévő adatkezelésből történő legyűjtés eredményeként létrejövő adatkezelés új adatkezelésnek számít, amennyiben az adatkezelés célja eltérően kerül megfogalmazásra, vagy az adatkezelő szervezeti egység megváltozik. Ilyen esetben erre vonatkozóan is bejelentési, illetve szabályzatkészítési kötelezettség lép életbe. Vitás esetben az adatvédelmi tisztviselő állásfoglalását kell kérni.

Az adatvédelmi tisztviselő gondoskodik a személyes adatkezelés nyilvántartásba vételéről és nyilvántartási számának visszajelzéséről az adatkezelő szervezeti egység számára. Ennek hiányában az adatkezelés nem kezdhető meg.

Amennyiben az újonnan létrehozott, vagy meglévő adatkezelés módosítása a munkavállalók nagyobb csoportját érintően a munkavállaló technikai ellenőrzését eredményezi, az adatvédelmi tisztviselő számára történő megküldést megelőzően, a Munkajog szervezet útján az adatkezelőnek ki kell kérnie a Központi Üzemi Tanács véleményét, egyben a Kollektív Szerződésben foglaltak szerint tájékoztatnia kell a szakszervezeteket.

Az adatkezelési nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység vezetője haladéktalanul, de legfeljebb 5 munkanapon belül köteles bejelenteni a Társaság adatvédelmi tisztviselőjének, aki ennek megfelelően módosítja az adatkezelési nyilvántartás adatait.

4.7.2 Adatvédelmi incidensek nyilvántartása

A bekövetkezett adatvédelmi incidensekről az Információ- és adatvédelem szervezet szakértője nyilvántartást vezet, az alábbi adattartalommal:

a) az érintett személyes adatok köre,
b) az adatvédelmi incidenssel érintettek köre és száma,
c) az adatvédelmi incidens időpontja,
d) az adatvédelmi incidens körülményei, hatásai,
e) az adatvédelmi incidens orvoslására megtett intézkedések,
f) az adatkezelést előíró jogszabályban meghatározott egyéb adatok.

4.8 Adatbiztonsági intézkedések

A személyes 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 munkahelyi vezető és a Biztonsági főigazgatóság alkalomszerűen ellenőrzi.

Tiszta asztal

a) A személyes adatokat tartalmazó papír alapú, valamint számítógépes adathordozók, hordozható számítógépek illetéktelen személy számára hozzáférhető módon, felügyelet nélkül nem hagyhatók.
b) Ahol zárható széfek, iratszekrények, fiókok, szekrények nem állnak rendelkezésre, a felügyelet nélkül hagyott iroda ajtaját minden esetben be kell zárni, oda illetéktelen személy bejutását egyéb technikai és szervezési intézkedésekkel meg kell akadályozni.
c) A munkaidő végén valamennyi személyes adatot tartalmazó adathordozót (notebook, pendrive, iratgyűjtő dosszié stb.) el kell zárni (pl. széf, lemezszekrény, egyéb zárható bútor), vagy megfelelő technikai intézkedéssel meg kell akadályozni az illetéktelen személy számára az adathoz való hozzáférést, valamint az azt hordozó eszköz eltulajdonítását (pl. Kensington zár).
d) 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.
e) A személyes adatok tárolására, elhelyezésre, feldolgozására szolgáló irodahelyiséget még az ideiglenes távollét idejére is be kell zárni.

f) A személyazonosító információkat (pl. telefonjegyzék, címjegyzék, naptár bejegyzések) oly módon kell elhelyezni, hogy azok tartalmát illetéktelenek ne ismerhessék meg.

Tiszta képernyő

a) A személyes adatokat tartalmazó, bekapcsolt állapotú számítógép felhasználója a munkaszoba ideiglenes elhagyása esetén zárolja a számítógépét a „Windows" valamint az „L" billentyű egyidejű lenyomásával, vagy jelentkezzen ki a felhasználói fiókjából (pl. CTRL-ALT-DEL egyidejű megnyomását követően a Kijelentkezés lehetőséget választva).

b) A személyes adatok feldolgozására alkalmazott számítógép képernyőjét az alábbi módszerek valamelyikének alkalmazásával védeni szükséges a jogosulatlan rálátás, betekintés elől:

- a munkaasztalok megfelelő elhelyezésével, elfordításával
- paraván alkalmazásával
- a helyiségbe történő belépés korlátozásával
- olyan technikai eszköz felszerelésével, ami a betekintési szöget jelentősen korlátozza
- a betekintés ideiglenes korlátozására az a) pontban leírt módszer is alkalmazható.

c) Amennyiben ezen módszerekkel nem akadályozható meg a betekintés, illetve a helyiségbe rendszeres munkavégzésre beosztott más munkavállaló illetéktelen betekintése, abban az esetben az adatvédelmi szabályok megismertetésével, szükség esetén titoktartási nyilatkozat kitöltésével kell biztosítani az adatok megfelelő védelmét.

A személyes adatok feldolgozására szolgáló alkalmazásokat úgy kell kialakítani, hogy az adatok megjelenítése során a monitoron figyelmeztető jelzés utaljon a tartalom zárt kezelést igénylő jellegére (pl. figyelmeztető felirattal vagy figyelemfelkeltő szín, effektus használatával). A korábban kifejlesztett alkalmazások korrekciója során gondoskodni kell az előzőkben írtak szerinti megoldás megvalósításáról.

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

4.8.1 Álnevesítés és anonimizálás

Az álnevesítés és az anonimizálás célja – az adattakarékosság hatékony megvalósítása érdekében – az adatvédelmi követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelési folyamatba.

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.

Álnevesítés esetén az azonosító mezőket egy vagy több mesterséges azonosítóval kell helyettesíteni.

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 álnevesítés (pszeudonimizáció) a személyes adatok olyan módon történő kezelése, amelynek következtében további információ felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni. 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. Az adatkezelő szervezeti egységeknek az elszámoltathatóság alapelvére figyelemmel is célszerű alkalmazniuk az álnevesítést, mint az adatok biztonságos kezelésének egyik eszközét, különösen olyan esetekben, amikor az adatkezelés valamilyen okból valószínűsíthetően magasabb kockázattal járhat az érintettekre nézve.

A személyes adatokat tartalmazó dokumentumok álnevesítésének, anonimizálásának gyakorlati alkalmazásához iránymutatás a 7.01-es mellékletben található.

4.8.2 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.

A biztonság megfelelő szintjének meghatározásakor tekintettel kell lenni az adatkezelésből eredő olyan kockázatokra, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

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.

Az adatok technikai védelmének biztosítása érdekében a Társaságnak, az általa megbízott adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének meg kell tennie az IBSZ előírásai szerinti védelmi intézkedéseket.

Az adatkezelés módjának meghatározásakor, valamint az adatkezelés során olyan technikai és szervezési intézkedéseket – például álnevesítést – kell végrehajtani az adatkezelőnek, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az általános adatvédelmi rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

4.8.3 Az adatok visszavonhatatlan 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, flash (NAND) 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. Az adathordozók megsemmisítését ellenőrizni, dokumentálni kell, valamint a dokumentációt a mindenkor hatályos iratkezelési szabályzatnak megfelelően kell kezelni és megőrizni.

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

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.

Amennyiben a helyreállíthatatlan törlés informatikai okból nem kivitelezhető, 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.

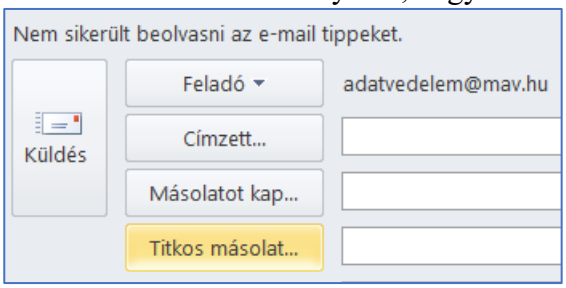
Amennyiben az adatok törlését jogszabály írja elő, de az az érintett jogos érdeke miatt ez nem lehetséges, a személyes adat kezelését (az adatot tartalmazó elektronikus vagy papír alapú

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 szekrényében kell megvalósítani.

Az adatkezelőnek olyan módon kell törölnie az érintett személyes adatát, hogy annak helyreállítása a továbbiakban ne legyen lehetséges, ezért nem elegendő a merevlemezek, illetve más informatikai adathordozók egyszerű formázása. Ennek a célnak bármely „HDD wipe" jellegű szoftver (pl. az ingyenes DBAN szoftver) megfelel. A személyes adatok törlését célszerű írásban, bizonyító erővel rendelkező módon (például az adatok törléséről készített jegyzőkönyvvel) dokumentálni. A jegyzőkönyvnek valamennyi olyan információt tartalmaznia kell, amely alapján bizonyítható, hogy az adatok törlése a jogszabályi előírásoknak megfelelően történt. Ennek keretében rögzíteni kell például a dokumentumban az olyan adatokat (pl. sorozatszám, IMEI szám), amelyek lehetővé teszik az adathordozó egyértelmű beazonosítását, továbbá a törlésre használt módszert. A törlési kötelezettség nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

4.8.4 Nagy mennyiségű címzett számára küldött üzenetek kezelése

Biztonsági okokból a Társaság levelező rendszeréből – alapértelmezés szerint – egyszerre legfeljebb száz címzett számára küldhető e-mail üzenet. Nagyobb címzetti kör számára küldendő üzenet esetén, különösen, ha a címzettek között nem kizárólag a MÁV-csoporthoz tartozó címzettek szerepelnek, az e-mail címek védelme érdekében az e-mail címeket a titkos másolat mezőben kell elhelyezni, hogy a címzettek egymás e-mail címét ne láthassák.



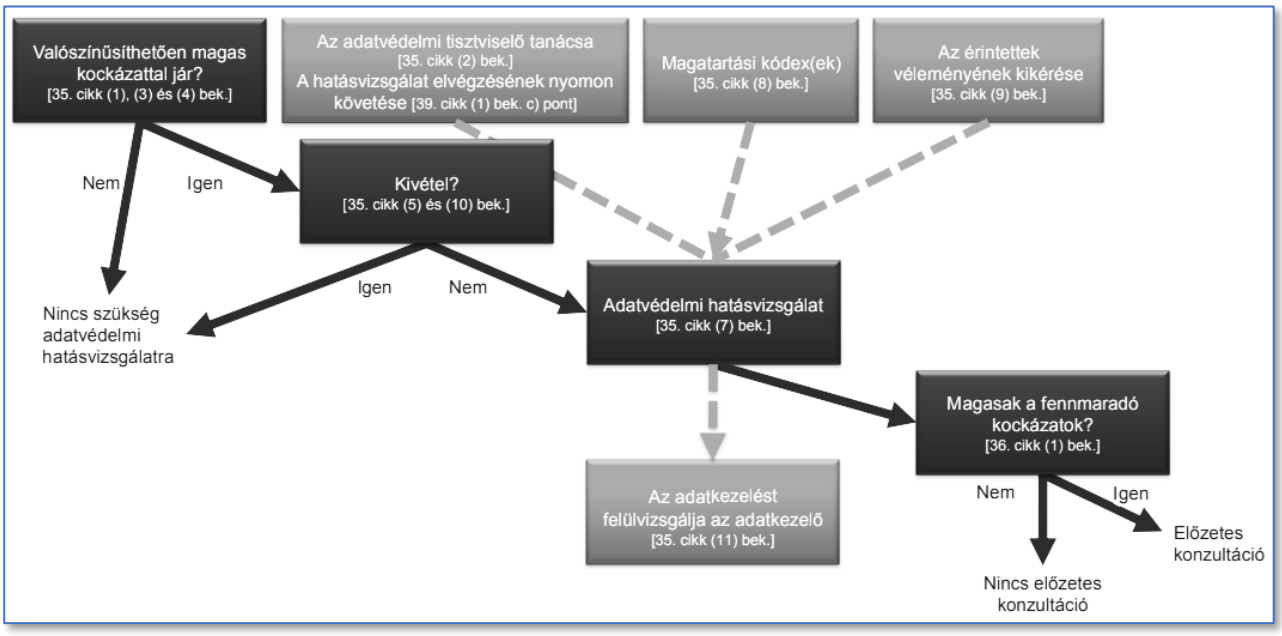
Amennyiben rendszeresen száznál több címzett számára szükséges üzenet küldése, úgy azt célszerű a szerveren létrehozott címlista segítségével megoldani. Erre nem vonatkozik a 100 címzettre vonatkozó limit, illetve nem eredményez adatvédelmi incidenst, ha a nagy mennyiségű címzetti kört tartalmazó címlista megnevezése nem a „Titkos másolat" mezőbe kerül beírásra.

4.8.5 Adatvédelmi hatásvizsgálat

Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját és mindezt megfelelően dokumentálja. Megkeresés esetén az adatvédelmi tisztviselő szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan.

Amennyiben az adatkezelés jellege, hatóköre, körülménye vagy célja valószínűsíthetően magas kockázattal jár, akkor az adatkezelést megelőzően hatásvizsgálatot kell végezni arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Ez különösen az automatizált adatkezelésen (pl. profilalkotáson) alapuló, a személyes adatok különleges kategóriáira, illetve a nyilvános helyek nagymértékű, módszeres megfigyelésére vonatkozó adatkezelések esetében kötelező. Annak eldöntéséhez, hogy szükséges-e hatásvizsgálatot végrehajtani, figyelembe kell venni az általános adatvédelmi rendelet előírásait, valamint azon adatkezelési műveletek listáját, amely a NAIH honlapján közzétett hatásvizsgálati jegyzékében szerepel. Az egymáshoz hasonlóan magas kockázatokat jelentő adatkezelések egyetlen hatásvizsgálat keretei között is értékelhetőek.

Arra vonatkozóan, hogy mely esetekben szükséges adatvédelmi hatásvizsgálat lefolytatása, illetve a felügyeleti hatóság véleményének kikérése, az alábbi ábra nyújt eligazítást:



Adatvédelmi hatásvizsgálat szükségességének megállapítása a GDPR alapján

Az adatvédelmi hatásvizsgálat elvégzésekor az adatkezelő köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát.

A hatásvizsgálatnak legalább az alábbiakra kell kiterjednie:

a) a tervezett adatkezelési műveletek módszeres leírása és az adatkezelés céljainak ismertetése, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálata;
c) az érintett jogait és szabadságait érintő kockázatok vizsgálata;
d) a kockázatok kezelését célzó intézkedések bemutatása, ideértve a személyes adatok védelmét és az általános adatvédelmi rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

Nem kell adatvédelmi hatásvizsgálatot végezni, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez, vagy közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, és az adatkezelést jogszabály írja elő, amennyiben a jogalkotó a jogszabály-előkészítés során adatvédelmi hatásvizsgálatot végzett.

Az adatkezelőnek szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést kell lefolytatnia annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

A hatásvizsgálatra vonatkozó kérdőív a 7.11 számú mellékletben található.

4.8.6 Érdekmérlegelési teszt lefolytatása

A jogos érdeken alapuló adatkezelés nem teszi szükségessé az érintett hozzájárulását, helyette az adatkezelés szükségességét és adatalany jogait és szabadságait teszi mérlegre. Az adatkezelő szükségesség-arányosság teszt végrehajtásával mutatja be, hogy az érintett adatvédelmi jogai miként viszonyulnak a személyes adatok kezeléséhez fűződő adatkezelői, illetve társadalmi jogi érdekekhez. Ez alapján az adatkezelő maga mérlegeli és dönti el, hogy az érintettek irányában miként tesz eleget az adatvédelmi szabályokban meghatározott kötelezettségeinek.

A jogos érdeken alapuló adatkezelés alkalmazásával együtt járó adatkezelési körülményeket az adatkezelőnek írásban rögzítenie szükséges annak érdekében, hogy az érintettek meg tudjanak győződni arról, hogy a szóban forgó adatkezelés valóban arányosan korlátozza a jogaikat.

Az érdekmérlegelési teszt elvégzése során az alábbi lépéseket célszerű követni.

1. lépés: az adatkezelés megkezdése előtt át kell tekinteni, hogy a cél elérése érdekében feltétlenül szükséges-e személyes adatok kezelése, rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adat kezelése nélkül megvalósítható a tervezett cél (cél teszt).
2. lépés: a Társaság részéről az adatkezelésre vonatkozóan felmerült jogszerű érdekeinek lehető legpontosabb meghatározása (szükségességi teszt).
3. lépés: annak kifejtése, hogy mi az adatkezelés célja, milyen személyes adatok, mennyi ideig tartó adatkezelését igényli a jogos érdek.
4. lépés: az adott adatkezelés vonatkozásában az érintettek érdekeinek meghatározása (pl. azok az ellenérvek, amelyeket a munkavállalók felhozhatnának az adatkezeléssel szemben).
5. lépés: annak meghatározása, hogy miért korlátozza arányosan a jogos érdek – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott érintetti jogokat, várakozásokat (arányossági teszt).
6. további lépés: amennyiben az elvégzett érdekmérlegelési teszt alapjául szolgáló adatkezelés valamely lényeges elemben megváltozik, az érdekmérlegelési tesztben foglaltakat szükséges felülvizsgálni annak megállapítása céljából, hogy az adott adatkezelés tekintetében a Társaság érdeke a körülmények módosulását követően is elsőbbséget élvez-e az érintettek alapvető jogai illetve szabadságai viszonylatában.

Az érdekmérlegelési teszt elvégzésre a 7.12 számú mellékletben található kérdőíves minta is felhasználható. A kitöltött teszt egy példányát – az adatkezelés nyilvántartásához kapcsolódóan – meg kell küldeni az adatvédelmi tisztviselő számra.

4.9 A munkavállalók személyes adatainak kezelése

A munkavállalók személyes adatainak a foglalkoztatással összefüggő kezelésére vonatkozóan jogszabály vagy kollektív szerződés olyan konkrét szabályokat írhat elő, amelyek meghatározzák a kötelezettségek teljesítését, a munka irányítását, tervezését és szervezését, a munkahelyi egyenlőséget és sokszínűséget, a munkahelyi egészségvédelmet és biztonságot, továbbá a foglalkoztatáshoz kapcsolódó jogok és juttatások egyéni vagy kollektív gyakorlását és érvényesülését, valamint a munkaviszony megszüntetése céljából történő adatkezelést.

Amennyiben a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelőnek az adatkezelés megkezdésétől legalább háromévente felül kell vizsgálnia, hogy az általa, illetve adatfeldolgozója által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. A felülvizsgálat körülményeit és eredményét dokumentálnia kell, és azt tíz évig meg kell őriznie, amelyet a felügyeleti hatóság kérésére rendelkezésére kell bocsájtania.

A munkavállalók személyes adatainak kezelése csak meghatározott, törvényes, arányos és szükséges célból történhet. Az adatok kezelésének a törvényes cél szempontjából megfelelőnek, relevánsnak és szükséges mértékűnek kell lennie. A jogalaptól függetlenül alkalmazni kell az arányosság és a szubszidiaritás elvét, vagyis azt a szempontot, hogy minden kérdést lehetőleg a legalacsonyabb szinten kell kezelni, minél közelebb ahhoz a közeghez, ahol az felmerül. A munkavállalók technikai megfigyelésével összefüggésben a technológia alkalmazását és célját átláthatóan kell megvalósítani. Az érintettek számára biztosítani kell, hogy gyakorolhassák jogaikat, beleértve a személyes adataikhoz történő hozzáférést, az azok helyesbítéséhez, törléséhez és korlátozásához való jogukat. Gondoskodni kell az adatok pontosságáról, és az adatoknak kizárólag a szükséges ideig történő megőrzéséről. Minden szükséges intézkedést meg kell tenni az adatok jogosulatlan hozzáférés elleni védelme érdekében, és biztosítani kell, hogy az érintettek tisztában legyenek az adatvédelmi kötelezettségeikkel.

A munkavállaló személyes adatainak kezelése az általános adatvédelmi rendelet szerinti jogalapok valamelyikének alkalmazásával lehetséges. Az egyenlőtlen viszony jellegéből adódóan azonban az adatkezelés jogalapjául – a legtöbb esetben – az érintett hozzájárulásától eltérő jogalapot kell használni, mert az érintett hozzájárulására, mint jogalapra kizárólag abban az esetben lehet hivatkozni, ha az adatkezelés során a munkavállaló feltétel nélküli előnyöket szerez, és őt semmiféle hátrány nem éri az adatkezelés megtagadása esetén. Az adatkezelés történhet a szerződés teljesítése

jogalapra történő hivatkozással, amennyiben ilyen kötelezettség teljesítéséhez a munkavállaló személyes adatait kezelni szükséges. A munka törvénykönyve és az egyéb foglalkoztatási jogszabályok olyan jogi kötelezettségeket írhatnak elő, amelyek személyes adatok kezelését teszik szükségessé. A munkáltató jogos érdeke alapján történő adatkezelés esetén jogszerű célt, a választott módszert, vagy technológiát szükséges és arányos módon kell meghatározni, és azt úgy kell alkalmazni, hogy a lehető legkisebb mértékben sértse a munkavállaló magánszféráját. Megfelelő intézkedésekkel biztosítani szükséges az egyensúlyt a munkavállalók alapvető jogai és szabadságai tekintetében.

Az adatkezelési műveleteknek meg kell felelniük az átláthatóság követelményeinek, és a munkavállalókat egyértelműen és teljes körűen tájékoztatni kell a személyes adataik kezeléséről, valamint megfelelő műszaki és szervezeti intézkedéseket kell tenni az adatkezelés biztonságának biztosítására.

4.9.1 Adatkezelés a munkaviszony létesítését megelőzően

A Társaság által közzétett álláshirdetésekben a Társaság megnevezése és elérhetősége (e-mail-cím, telefonszám) feltüntetése szükséges, amelyek segítségével a pályázó a személyes adatai kezelésével összefüggésben gyakorolhatja jogait, így például kérheti személyes adatainak törlését.

A jelentkező vonatkozásában csak olyan adat benyújtása kérhető, illetve olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely a munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges. Olyan személyes adatok, mint például a pártállás, érdekképviseleti szervezethez való tartozás, vallási meggyőződés, vagy a pályázó fényképe, nem kezelhetők.

A kiválasztási eljárás során a közösségi oldalak megtekintésével összefüggésben az alábbi adatvédelmi követelmények betartása szükséges:

- amennyiben a kiválasztási eljárás során megtekintik a pályázó valamely közösségi oldalon létrehozott profilját, azt előzetesen ismertetni szükséges;
- az adott álláspályázat kapcsán kizárólag a lényeges, releváns, a pályázó által nyilvánosan közzétett adat ismerhető meg, zárt csoport más tagja által megszerzett adat nem;
- a pályázó közösségi oldalon nyilvánosan végzett tevékenysége megismerhető, abból következtetés vonható le, de további adatkezelés pl. a pályázó profiloldalának eltárolása, vagy továbbítása nem megengedett.

A pályázat lezárását követően valamennyi pályázó kiértesítése szükséges. A ki nem választott pályázók személyes adatait törölni kell, illetve amennyiben a pályázó kéri, úgy a pályázati anyagát vissza kell küldeni részére. A kiválasztás lezárásakor törölni kell a pályázóról készített feljegyzéseket is. A pályázatok jogszerű további kezeléséhez kizárólag a pályázó önkéntes, konkrét és megfelelő tájékoztatáson alapuló, egyértelműen kinyilvánított hozzájárulása esetében, észszerű ideig van lehetőség. A pályázó büntetlen előélete igazolására vonatkozóan a Hatósági erkölcsi bizonyítványok kezelése (4.1.12.1) pontban meghatározottakra figyelembe kell eljárni.

4.9.2 Adatkezelés a munkaviszony létesítése, fennállása során

A munkáltató az adatkezeléséről az érintettet köteles írásban tájékoztatni. A munkáltató a munkavállalótól olyan nyilatkozat megtételét vagy személyes adat közlését követelheti, amely a munkaviszony létesítése, teljesítése, megszűnése (megszüntetése) vagy az Mt.-ből származó igény érvényesítése szempontjából lényeges, továbbá azokat – a munkavállaló előzetes tájékoztatása mellett – adatfeldolgozó számára átadhatja. A munkáltató kérheti a munkaviszonnyal összefüggően okirat bemutatását, azonban erről másolatot nem készíthet.

A munkaviszony létesítésére vonatkozó adatkezelési szabályok az irányadók abban az esetben, amennyiben a munkakör megváltozása vagy a fennálló munkaviszony egyéb elemeinek megváltozása miatt válik szükségessé a munkavállaló személyes adatainak pontosítása vagy kiegészítése.

A munkavállaló vonatkozásában csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely a munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.

4.9.3 Adatkezelés a munkaviszony megszűnését követően

A Társaság a munkavállaló személyi anyagának megőrzésére jogi kötelezettség (törvény) alapján a következő körben köteles:

a) az adózás rendjéről szóló 2017. évi CL. törvény 78. § (4) bekezdése alapján a Társaság általa megállapított adó, adóelőleg alapjául szolgáló bizonylatokat az adó megállapításához való jog elévüléséig, a halasztott adó esetén a halasztott adó esedékessége naptári évének utolsó napjától számított öt évig köteles megőrizni;

b) a számvitelről szóló 2000. évi C. törvény 169. §-a alapján az üzleti évről készített beszámolót, az üzleti jelentést, valamint az azokat alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá a naplófőkönyvet, a könyvviteli elszámolást közvetlenül és közvetetten alátámasztó számviteli bizonylatot vagy más, a Számv. tv. követelményeinek megfelelő nyilvántartást olvasható formában legalább 8 évig köteles megőrizni;

c) azon iratok megőrzése, amelyek a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény 3. § j) pontja szerint maradandó értékű iratnak minősülnek, a Társaság kötelezettsége a munkaviszony megszűnése után is;

d) a Társaság a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény szerint a foglalkoztatott biztosítási jogviszonyával összefüggő, a szolgálati időről vagy a nyugellátás megállapítása során figyelembevételre kerülő keresetről, jövedelemről adatot tartalmazó munkaügyi iratokat a foglalkoztatottra irányadó öregségi nyugdíjkorhatár betöltését követő 5 évig köteles megőrizni.

Azon személyes adatokat, amelyek esetében a kezelést, illetve tárolást jogszabályi kötelezettség nem írja elő, vagy eltérő adatkezelési jogalap nem teszi lehetővé, törölni kell.

A munkaviszony megszűnését, megszüntetését követően a munkavállalónak a Társaság infokommunikációs rendszeréhez történő hozzáférését haladéktalanul meg kell szüntetni. A levelező rendszerben átmenetileg automatikus tájékoztatás segíti a levél küldőjét abban, hogy a jövőben a megszüntetett postafiók helyett ügyintézés céljából mely címzett fogadja a levelét.

4.10 A munkavállaló ellenőrzésével összefüggő adatkezelés

A munkáltató a munkavállalót a munkaviszonnyal összefüggő magatartásával összefüggésben ellenőrizheti. Az ellenőrzési jog rendeltetésszerűen gyakorolható, ami nem irányulhat vagy vezethet mások jogos érdekeinek csorbítására, érdekérvényesítési lehetőségeinek korlátozására, zaklatására, véleménynyilvánításának elfojtására.

A munkavállaló személyiségi joga az ellenőrzéssel annyiban korlátozható, amennyiben a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos.

Ha az ellenőrzés a munkavállaló személyiségi jogait korlátozza az alábbi jogkorlátozási teszt végrehajtásával állapítható meg, hogy a munkavállaló munkaviszonnyal összefüggő magatartásának ellenőrzése a személyiségi jogokat az Mt.-vel összhangban korlátozza-e. Ennek során vizsgálni szükséges, hogy az ellenőrzés

- a munkavállaló mely személyiségi jogait korlátozhatja, illetve korlátozza;
- a korlátozás a munkaviszony rendeltetésével közvetlenül összefügg-e;
- a munkaviszony teljesítéséből nyilvánvalóan következő okból történik-e,
- ezen ok alapján a munkavállaló személyiségi jogainak korlátozása feltétlenül szükséges-e;
- más kevésbé korlátozó eszköz áll-e rendelkezésre;
- az ellenőrzés a cél elérésével arányos-e;
- az ellenőrzés a célhoz képest nem túlzó-e.

Az adott eset konkrét körülményeinek átfogó és összegző értékelésével lehet dönteni arról, hogy a jogkorlátozás adott esetben megengedett-e. A korlátozás módjáról, feltételeiről és várható tartamáról, továbbá azon technikai eszközök alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak a munkavállalót előzetesen tájékoztatni kell.

Az ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló munkaviszonnyal összefüggő magatartása a munkavállaló magánélete tiszteletben tartásával ellenőrizhető.

Ha az ellenőrzés és az ahhoz kapcsolódó adatkezelés a munkavállaló személyiségi jogait korlátozza, az akkor jogszerű, ha

- a munkáltató az ellenőrzési jogát rendeltetésszerűen gyakorolja,
- az ellenőrzés a munkavállaló munkaviszonnyal összefüggő magatartására irányul, nem a magánéletére,
- az ellenőrzés nem sérti a munkavállaló emberi méltóságát,
- a munkavállaló személyiségi jogait az Mt. 9. § (2) bekezdésével összhangban korlátozza,
- az adatkezelés jogalapja megfelelő,
- az adatkezelés az adatvédelmi alapelvekkel összhangban van,
- az ellenőrzésről, illetve adatkezelésről, annak időpontjáról vagy időtartamáról a munkáltató megfelelően tájékoztatta a munkavállalót az Mt. és a GDPR rendelkezései szerint.

A munkavállaló munkaviszonnyal kapcsolatos magatartása különböző módokon ellenőrizhető. A következőkben a technikai eszközzel vagy elektronikus úton, valamint a személyesen végzett ellenőrzés esetei közül azokat mutatjuk be, amelyek korlátozhatják a munkavállaló személyiségi jogait és szükségszerűen együtt járna a munkavállaló személyes adatainak kezelésével.

4.10.1 Az informatikai eszközök használata, naplózása, ellenőrzése

A munkavállaló által használt informatikai eszközök jogszerű ellenőrzésének előfeltétele az, hogy az ellenőrzés pontos részleteiről, az ellenőrzést megelőzően megfelelő formában és módon tájékoztatást kell adni a munkavállalók számára. A tájékoztatásnak ki kell terjednie különösen arra, hogy az adatkezelés milyen célból és milyen jogalappal történik, ki az adatkezelő, mennyi ideig kezelik a felvett adatokat, illetőleg az adatkezeléssel kapcsolatban milyen jogai vannak az érintett személyeknek.

A Társaság a munkavállalók részére a munkakörök ellátásához, kizárólag munkavégzés céljára asztali számítógépet, hordozható informatikai eszközt, központi tárhelyet, internet-hozzáférést, elektronikus postafiókot, okostelefont, vezetékes üzemi, illetve közcélú távközlési hálózat igénybevételét lehetővé tevő telefont biztosíthat (a továbbiakban: infokommunikációs eszköz). Az informatikai biztonság szintjének fenntartása, illetve a használati előírások betartásának kontrollja érdekében ezen eszközök és szolgáltatások használatával kapcsolatos forgalmi adatokat a Társaság naplózza és az azokban szereplő adatokat ellenőrzi. Az ellenőrzésre szolgáló technikai eszközök és biztonsági rendszerek alkalmazásáról a munkavállalókat a MÁV Zrt. védendő információinak kezeléséről szóló EVIG utasítás 2. számú melléklete szerinti információvédelmi nyilatkozat, illetve az általános munkavállalói adatkezelési tájékoztató útján tájékoztatni kell. Az információvédelmi nyilatkozat egyesítve tartalmazza az informatikai biztonságra, a védendő információkra vonatkozó részeket, amelynek egy aláírt példányát a munkavállaló humán dokumentumai között kell elhelyezni.

Az infokommunikációs eszközök ellenőrzésének indokolt esetei

Az infokommunikációs eszközök előzőekben bemutatott ellenőrzésén túl a Társaság – különösen az alábbi indokolt esetekben – további ellenőrzést folytathat le, az adott ellenőrzéssel érintett munkavállaló tájékoztatása mellett:

- a munkavállaló infokommunikációs eszköz használatánál a számára engedélyezett költségkeretet indokolatlanul túllépi,

- a munkavállaló a MÁV Zrt. védendő információinak kezeléséről szóló EVIG utasítás szerinti védendő információt arra illetéktelen személlyel, vagy szervezettel megosztja vagy megoszthatja,
- amennyiben az adatok kiadása az érintett vagy egy másik természetes személy létfontosságú érdekei védelméhez szükséges, és – különleges személyes adatok esetén – az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni, egyúttal a jogi cselekvőképtelenség megítélése tekintetében a Jogi főigazgatóság egyetért (létfontosságú érdekre hivatkozással történhet az adatkezelés pl. humanitárius katasztrófák esetében, ideértve, azt az esetet is, ha arra a járványok és terjedéseik nyomon követéséhez van szükség; más természetes személy létfontosságú érdekeire hivatkozással személyes adatkezelésre akkor kerülhet sor, ha az adatkezelés egyéb jogalapon nem végezhető),
- minden olyan körülmény, amely alapján alappal feltételezhető, hogy a munkavállaló az általában elvárható etikai normák súlyos megszegésével járt el; az információs önrendelkezési jog korlátozásával arányosság megítélése tekintetében ki kell kérni az adatvédelmi tisztviselő tanácsát.

Az infokommunikációs eszközök és szolgáltatások rendeltetésszerű használatára fel kell hívni a munkavállalók figyelmét, beleértve azt is, hogy az eszköz használata önmagában megteremti annak lehetőségét, hogy az abban rögzített adatokat a munkáltató, a jogszabályi előírásoknak és jelen szabályzatnak megfelelően felhasználja, és annak használatát ellenőrizze. Az infokommunikációs eszközök használatát szabályozó előírások megsértése, vagy annak veszélye esetén – indokolt esetben – tájékoztatni kell a munkáltatói jogkörgyakorló vezetőt, aki az adatvédelmi tisztviselő és a biztonsági szervezet egyidejű tájékoztatása mellett, az illetékes rendszergazda, illetve amennyiben az informatikai biztonság veszélyeztetése is felmerül az Információ- és adatvédelem szervezet bevonásával külön eseti ellenőrzést rendelhet el. A vizsgálat során biztosítani kell a munkavállaló személyes (vagy ha ez nem biztosítható, meghatalmazottja, képviselője) jelenlétének lehetőségét.

Kizárólag rendkívüli esetekben fogadható el, hogy az ellenőrzésnél a munkavállaló ne legyen jelen, például azonnali intézkedést igénylő esetekben, vagy betegállományban lévő munkavállaló esetében nem halasztható intézkedés alkalmával. Ebben az esetben is meg kell kísérelni a tájékoztatást nyújtását a munkavállaló számára a tervezett munkáltatói intézkedésről, amelyben lehetőséget kell biztosítani a meghatalmazotti vagy képviselő jelenlétére az ellenőrzésnél.

Az ellenőrzés tényét, helyét, idejét, indokát, eredményét, valamint a résztvevők nevét és munkakörét jegyzőkönyvben kell rögzíteni.

A munkáltató eseti ellenőrzésének megvalósítására a munkavállaló tájékoztatását követően kerülhet sor, amelynek során ügyelni kell a fokozatosságra, figyelemmel arra, hogy milyen információk állnak a munkáltató rendelkezésére, ugyanis ezek az információk befolyásolhatják az ellenőrzés fókuszát, menetét.

Amennyiben ezen megelőző intézkedések – előzetes tájékoztatás és a munkavállaló vagy meghatalmazottja, képviselője jelenlétének biztosítása – ellenére a munkavállaló nem érhető el vagy nem jelenik meg sem személyesen, sem képviselője útján, akkor távollétében, független harmadik személy alkalmazásával is hozzá lehet férni az infokommunikációs eszközeihez az ellenőrzés, illetve az azonnali intézkedések végrehajtása érdekében. Ilyen esetben is meg kell tenni mindent annak érdekében, hogy az ellenőrzés körülményei olyan módon legyenek jegyzőkönyvben rögzítve (adott esetben az ellenőrzés eredményében nem érdekelt személyek mint hitelesítő személyek jelenléte mellett vagy más megfelelő módon), hogy annak pontos menete, az annak során megismert adatok köre, azaz a ténylegesen elvégzett adatkezelési műveletek és azok jogszerűsége utólag ellenőrizhető legyen.

A leadott, de a Társaságon belül továbbhasznosításra kerülő mobiltelefon készülékről a személyes adatokat a gyári állapot visszaállításával törölni szükséges. A használatból végleges kivonás esetén, gondoskodni kell az adatok visszaállíthatatlan módon történő megsemmisítéséről.

4.10.2 Elektronikus levelezés

Az elektronikus levelet azonos szintű védelemben kell részesíteni, mint a hagyományos, postai úton továbbított küldeményt. A Társaság megbízásából, a munkavállaló által hivatalos ügyekben írt és fogadott elektronikus dokumentum tartalmát a munkáltatói jogkörgyakorló, illetve a Társaság szabályzataiban meghatározott szervezet, vagy személy jogosult megismerni, ugyanakkor biztosítani kell a levelezésben érintett harmadik személy azon jogát is, hogy az adatkezelés részleteiről tájékoztatást kapjon.

A Társaság által biztosított elektronikus levelező rendszer használata során, a személyes adatok védelme érdekében különösen az alábbi szabályokat kell betartani:

a) a levelező rendszer hivatalos célra használható;
b) a nagyszámú, különösen az egyedi engedély alapján lehetővé tett több mint száz e-mail címzett megadása esetén a küldemény valamennyi címzettjét rejtett módon (titkos másolat mezőben) kell megadni;
c) amennyiben a címzettek között a Társaság levelezőrendszerén kívüli címzett is szerepel, adatvédelmi szempontból is fokozottan vizsgálni kell a b) pontban leírt módszer alkalmazásának szükségességét;
d) a Társaság hivatalos elektronikus levelezésben a QR kódnak a Társaság munkavállalója által küldött e-mail aláírásában történő felhasználása nem megengedett;
e) a nagyobb mennyiségű személyes adatot tartalmazó elektronikus küldemény informatikai rendszer útján továbbítása kizárólag technikai védelemmel (illetéktelen megnyitás ellen jelszóval védett Office dokumentumban, RMS védelemmel, jelszóval védett tömörített állományban stb.) engedélyezett;
f) a személyes adatot tartalmazó elektronikus leveleket 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 feladójával és az üzenetet haladéktalanul törölje a számítógépéről. A levél feladójának e-mail címe kifejezetten vállalati felhasználásra szolgál, a biztonsági szervezet – vezetői ellenőrzés céljából – betekinthet tartalmába, kérem erre a címre magánjellegű küldeményt, reklámanyagot ne küldjön!”

A munkáltató nem jogosult az e-mail-fiókban tárolt magánjellegű e-mailek tartalmát ellenőrizni még akkor sem, ha az ellenőrzés tényéről előzetesen tájékoztatta a munkavállalót.

Amennyiben az ellenőrzés pusztán arra terjed ki, hogy megállapítsa azt, hogy a munkavállaló betartotta-e ezt a munkáltatói rendelkezést, akkor elegendő az email címének és tárgyának megtekintése, és nem szükséges a levél tartalmának megismerése.

Amennyiben a felhasználó munkavégzésre irányuló jogviszonya megszűnik, az informatikai hálózathoz hozzáférési jogosultságait (így különösen az AD tagságát) és a rendelkezésére bocsátott postafiókot a munkaviszony megszűnésével egyidejűleg fel kell függeszteni. Legkésőbb a felhasználó munkaviszonyának megszűnésétől számított három hónap elteltével, a felhasználó postafiókját és annak tartalmát törölni kell. A levelezésre használt infokommunikációs eszköz adattartalmára vonatkozóan a felhasználót a jelen utasítás 7.7 mellékletben található „*Nyilatkozat az infokommunikációs eszközök adattartalmáról az eszköz visszaszolgáltatásakor*” felhasználásával nyilatkoztatni kell. A munkáltatói jogkörgyakorló gondoskodik arról, hogy a kilépett felhasználó e-mail címére beérkező levelekre a feladónak automatikus tájékoztató e-mail kerüljön megküldésre, , indokolt esetben tájékoztatást adva arról, hogy az adott e-mail cím a továbbiakban nem elérhető és szükség szerint megadva a feladó számára azt, hogy az adott feladatkörben mely postafiók fogadja a leveleket elintézésre.

A védendő információk megóvása érdekében a Társaság adatszivárgás elleni védelmi rendszerrel monitorozza a levelező rendszeren keresztül a Társaság zárt hálózatát elhagyó küldeményeket. Az

adatkezelés adatvédelmi vonatkozásait az *Adatszivárgás elleni védelmi rendszer* (DLP) című fejezet tartalmazza.

A forgalmi szolgálattevők zárt csoportú e-mail rendszerének használatáról szóló utasítás hatálya alá tartozó, kizárólag vasútüzemi célú postafiókokat hivatalos közlemények továbbítására szabad használni, ezek kezelésére, ellenőrzésére az utasításban meghatározott speciális szabályok érvényesek.

4.10.3 Az internet használatának korlátozása

Az internethasználat ellenőrzéséhez a munkáltatónak olyan érdeke fűződik, mint például az adatbiztonság, a munkáltató erőforrásainak kímélete, üzemgazdasági, munkaszervezési szempontok érvényre juttatása, a munkavállaló munkavégzési kötelezettségének teljesítésével össze nem egyeztethető magatartások megelőzése.

A Társaság az internet hozzáférést munkavégzés céljából bocsájtja a munkavállalók rendelkezésére, annak magáncélból történő felhasználását pedig megtiltja. Az internethasználat szabályait, a használat biztonsági célból bevezetett korlátait az internet hozzáférés biztosításának és használatának szabályairól szóló elnök-vezérigazgatói utasítás tartalmazza. A munkavállalók internet használatának kontrollja úgy érvényesül, hogy az egyes oldalak megnyitását az informatikai rendszer segítségével korlátozza.

A vendégek, illetve a munkavállalók saját eszközeivel történő internet használatra a Társaság által – a technikai lehetőségek függvényében – biztosított vendég Wi-Fi (guest, BYOD) hozzáférés útján történő forgalmazás nem kerül naplózásra, mindössze a káros tartalmak elleni oldalakhoz történő hozzáférés korlátozással valósul meg.

4.10.4 Adatszivárgás elleni védelmi rendszer (DLP)

A munkavállaló köteles megőrizni a munkaköre betöltésével összefüggésben tudomására jutott védendő információt, amelynek közlése a munkáltatóra, vagy más személyre hátrányos következménnyel járhat.

Az információk kiszivárgásának elkerülése érdekében a Társaság adatszivárgás elleni védelmi rendszert (DLP) alkalmaz, amely átfogó monitorozási képességgel rendelkezik az informatikai hálózaton, valamint egyes magas kockázatúnak nyilvánított felhasználói számítógépeken egyaránt. A rendszer működtetése során kiemelt figyelmet kell fordítani a felhasználók személyes adatainak védelmére. A technikai ellenőrzésről szóló részletes szabályozásban valamennyi érdemi információra kiterjedően tájékoztatni kell a felhasználókat arról, hogy a számukra biztosított informatikai eszközökön a személyes használat nem engedélyezett, továbbá ismertetni kell számukra azt, hogy mely védett információk körének mozgását ellenőrzi a rendszer.

Az egyes munkafolyamatokat célzottan, előre leegyeztetett módon, valamennyi felhasználóra érvényesen és azonos módon kell monitorozni. A téves riasztások minimalizálása érdekében részletesen meg kell határozni az azonosítási technológiát, és mind a rendszerhez, mind annak naplóállományához történő hozzáféréseket a szükséges minimális jogosultság elvének betartásával kell megadni. Az adatszivárgási incidensek kivizsgálási folyamatát oly módon kell kialakítani, hogy a rendszer által megjelölt adatszivárgási események valósak és észszerű emberi ráfordítással feldolgozhatóak legyenek.

4.10.5 Mobil Device Management rendszer (MDM)

A Társaság az MDM rendszert a felhasználó által használt vállalati mobil eszközre (okostelefon, tablet) telepítve, legalább közepes, illetve annál magasabb biztonsági fokozatú védelem (PIN kód, jelszó stb.) használatának kikényszerítésével és szükség esetén titkosítással gondoskodik az eszköz védelméről, ugyanakkor a felhasználó nevén és e-mail címén kívül egyéb személyes adatot nem kezel. A rendszer biztonsági beállításait az MDM Rendszerszintű Biztonsági Szabályzata részletesen meghatározza. A személyes adatok védelme érdekében az adatvédelmi tisztviselő, illetve felhatalmazottja bármikor, folyamatában jogosult a Mobil Device Management rendszer adatvédelmet érintő beállításainak ellenőrzésére, illetve a rendszer felhasználói közvetlenül is megkereshetik őt az MDM rendszer adatvédelmi beállításaival kapcsolatos kérdéseikkel. Az

ellenőrizhetőség érdekében az MDM rendszer üzemeltetője a rendszer beállításainak változásait folyamatosan naplózza. A munkavállaló földrajzi helyzetének rögzítése

4.10.6 A munkavállaló által használt szolgálati gépjármű tartózkodási helyének rögzítése

A gépjárműbe szerelt GPS (Global Positioning System, Globális Helymeghatározó Rendszer) nyomkövető által közvetített adat a gépjárművet vezető, illetve az abban tartózkodó személy személyes adatának minősül. A munkavállaló tartózkodási helyének rögzítésére a Társaság erre alkalmas technológiát (pl. GPS műholdas helymeghatározás) alkalmaz.

GPS alkalmazása elsősorban logisztikai célból történik különösen abból a célból, hogy az a jármű helyzetének meghatározását szolgálja, ne pedig a munkavállaló követését. A munkavállaló által vezetett gépjármű használata során történő GPS adatok felvétele a munkavállalóval megkötött gépjármű használati megállapodásban rögzítettek szerint történik. Ebben a Társaság részletes tájékoztatást nyújt a tartózkodási hely rögzítésére alkalmas technológia alkalmazásáról és a rögzített adatok köréről. Minden használat megkezdésekor megkövetelt az érintettet azonosító kód megadása vagy a munkavállalóknak kiosztott elektronikus azonosító használata az adat megfelelő kezelése érdekében. A gépjármű magáncélú igénybevételére is feljogosított munkavállaló magáncélú használata során keletkezett személyes adatát a Társaság nem kezeli.

4.10.7 A fegyveres biztonsági őri feladatokat ellátó munkavállalók tartózkodási helyének rögzítése

A GPS alapú segélyhívó és járőrellenőrző rendszer (Kashmir) célja az emberi élet, testi épség és vagyon sérelmére elkövetett jogsértések bizonyítása, valamint a szolgálati tevékenység ellenőrzése. További cél a rendszert használó személyzet biztonságának növelése, az élőerős személyzet valós idejű irányítási hatékonyságának növelése, a gyors reagálás elősegítése, valamint a szolgálati idő alatti járőr-tevékenység monitorozása, ellenőrzése, amelyhez a rendszer, hely- és időadatokat gyűjt a kiadott kézi készülékek segítségével.

4.10.8 A távolról végzett munka / home office

A felhasználónak gondoskodnia kell arról, hogy a védendő információ ne kerüljön illetéktelen kezekbe. A munkáltató által biztosított eszközöket a Home Office keretében foglalkoztatott munkavállaló köteles rendeltetés szerint használni, azok épségére vigyázni, valamint illetéktelen személyektől távol tartani, azokat kizárólag a Home Office keretében foglalkoztatott munkavállaló használhatja. A munkavállalónak a munkavégzéshez használt informatikai eszközeit és a papír adathordozón lévő adatokat munkaidőn kívül zárható szekrényben kell tárolnia és az otthonról végzett munkavégzés során a védendő információ kezelésére különös gondot kell fordítania. Az erre a célra használt vállalati eszközön tárolt adatok megfelelő védelméről, a kijelzőn megjelenített adatok bizalmasságáról a felhasználónak minden esetben gondoskodnia kell.

4.10.9 A munkahelyi telefonhasználat ellenőrzése

A munkáltató jogosult a munkavállaló rendelkezésére bocsátott telefon használatát ellenőrizni, amely során meg kell felelnie az adatvédelmi jogszabályok által támasztott követelményeknek.

A munkavállaló által lefolytatott telefonbeszélgetések mind a hívott, mind a hívó fél személyes adatának minősülnek, ezért a munkáltató a munkavállaló által lefolytatott magánjellegű telefonhívások adatait nem jogosult kezelni.

A munkahelyi telefonhasználat ellenőrzésére az alábbi módszerek alkalmazhatók:

a) A munkavállaló által használt telefon híváslistája a munkavállalónak lezárt borítékban átadható (azt előzetesen a munkáltató nem kezelheti), amelyről érintett a magán hívások telefonszámait oly módon törli, hogy azokat a későbbiekben ne lehessen azonosítani. A fennmaradó munkacélú híváslista a munkáltató által kezelhető.
b) A hívható számok előzetesen korlátozhatók (fixlista beállítása).
c) A magánjellegű hívásokhoz előhívó kód rendelhető.

A telefonbeszélgetések lehallgatása – a forgalomtechnológiai okokból végzett hangrögzítés kivételével – tilos.

4.10.10 Forgalomtechnológiai okokból végzett hangrögzítés

A MÁV-csoport tulajdonában álló hangkommunikációs eszközökön (diszpécsertelefon, mozdonyrádió, GSM-R berendezés, illetve bármely más forgalomtechnológiai szolgálati célra használt eszköz) rögzítése, továbbá a forgalmi szolgálattevők szolgálati helyiségében szóban elhangzó közlemények adása során magáncélú beszélgetés tilos. A hangrögzítést és a rögzített anyag kezelését a forgalomszabályozásra használt, technológiai célú és utastájékoztató hangrögzítő rendszerek működtetésének feltételeiről szóló EVIG utasítás alapján kell végrehajtani. A Társaság munkavállalói számára a hangrögzítő rendszer alkalmazásáról történő tájékoztatás elektronikus hírlevélen keresztül történik. A vállalkozó vasúti társaságokkal a hálózat hozzáférési szerződésben szükséges a vasúti társaság kötelezettségvállalását rögzíteni arra vonatkozóan, hogy a hangrögzítés tényéről az érintett munkavállalóit előzetesen írásban, kimutatható módon tájékoztatja.

A Társaság területén forgalomtechnológiai okokból végzett hangrögzítés során a hangrögzítő berendezéseken rögzített adatokat a munkaterületen munkáltatói jogokat gyakorló, hatáskörileg illetékes vezető, és vasútbiztonsági ellenőrzés, vagy baleset esetén a balesetvizsgáló csoport vezetője, illetve az általuk meghatalmazott személy hallgathatja vissza. A hangfelvételek adathordozóra történő rögzítésére baleset vagy egyéb rendkívüli esemény miatt indult belső vizsgálat, illetve hatósági, bírósági eljárás keretében van lehetőség.

A szolgálati helyiségben alkalmazott hangrögzítő berendezést oly módon kell kialakítani és működtetni, hogy az csak az érdemi kommunikáció időtartama alatt működjön úgy, hogy arról a helyiségben tartózkodók számára figyelemfelhívó fényjelzés is tájékoztatást adjon. A Társaság az ezeken az eszközökön zajló teljes beszédforgalmat jogszabályi felhatalmazás alapján rögzíti és ellenőrzi. A használat szabályairól és használat ellenőrzése érdekében alkalmazott hangrögzítő berendezés használatáról a munkavállalókat írásban tájékoztatni kell a szolgálati helyiségben tájékoztató kifüggesztésével, a kiadott eszközök esetében a 7.2 számú mellékletben foglalt nyilatkozat kitöltésével, amelynek a munkavállaló által aláírt példányát a munkavállaló humán anyagai között kell elhelyezni.

4.11 Egyéb adatkezelések

4.11.1 Integrált Humán Információs rendszer (IHIR)

A munkavállalótól csak olyan adat közlése, vagy nyilatkozat megtétele kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.

Az IHIR rendszerben, valamint a személyügyi dossziéban elhelyezett adatok nyilvántartásának vezetéséhez az érintett munkavállaló saját magára vonatkozóan köteles adatot szolgáltatni. A munkaviszony létesítése, módosítása és megszüntetése munkafolyamatainak szabályozásáról a humánerőforrás szervezet gondoskodik. A nyilvántartás pontossága, teljessége, naprakészsége érdekében az érintett munkavállaló az adatkörében beállt változásról köteles írásban bejelentést tenni.

A törzsszám használatára vonatkozó főbb alapelvek:

a) olyan IHIR rendszer által generált belső azonosító, amely nem tartalmazhat az érintett munkavállalóval kapcsolatba hozható személyes adatot;
b) a törzsszámot a munkaviszonnyal összefüggésben, a Társaság, illetve az informatikai szolgáltató kezeli;
c) használata a munkaviszonnyal közvetlenül, vagy legalább közvetve összefüggő, az e státuszhoz kapcsolódó adatkezeléseknél megengedett;
d) amennyiben a törzsszám harmadik fél számára átadásra kerül, a kezelés feltételeit külön szerződésben kell meghatározni;
e) a munkavállalók azonosítása a törzsszám és név alapján történik, további személyazonosító adatok kezelése csak kifejezetten és külön megindokolt esetben megengedett.

Az informatikai szolgáltató által telefonon biztosított helpdesk szolgáltatás igénybevétele esetén a hívó fél telefonon történő azonosítása szükséges, amelynek során biztosítani kell, a visszaélés lehetőségének kizárását. Ennek során a helpdesk kérheti az ügyfél azonosításához feltétlenül

szükséges személyes adatait, illetve az ügyfél azonosításának egyéb módja is lehetséges, például az ügyfél-, vagy törzsszámnak tone üzemmódú telefonon történő begépelése alapján. Amennyiben az ügyfél nincs meggyőződve arról, hogy kinek adja meg azonosító adatait, vagy nem kívánja személyes adatait telefonon megadni, elektronikus levélben, esetlegesen személyesen is felveheti a kapcsolatot a helpdeskkel.

A munkavállalók humán adataihoz történő belépési-, betekintési- és hozzáférési jogosultságokat munkakörhöz igazítottan, a munkavégzés megfelelő ellátásához szükséges legkisebb mértékű jogosultsági szinten kell meghatározni. Az adatokhoz történő hozzáférést, az azokkal végzett műveleteket – a rendszer lehetőségeinek határain belül – részletesen naplózni kell. A közvetlen munkahelyi vezetők felelősségi körébe tartozik a jogosultságok fentiek szerint meghatározott legkisebb mértékű használatának biztosítása és a hatáskörtúllépés kizárása, ennek ellenőrzése, naprakészségének biztosítása, a jogosultságok beállításának, módosításának, visszavonásának kezdeményezése.

4.11.2 A munkahelyre érkező magánjellegű küldemények kezelése

Magánjellegű levelezés folytatása a Társaságnál nem engedélyezett. Amennyiben ennek ellenére postai, vagy futár útján ilyen névre szóló küldemény érkezik, annak felbontása nem csak az érintett személyes adatai védelméhez, hanem a levéltitokhoz való jogának sérelmével is járhat, ezért azt más nem bonthatja fel, a címzettnek át kell adni, vagy a feladójának vissza kell küldeni. Amennyiben kétség merül fel a levél hivatalos, vagy magánjellegét illetően, a címzett számára lehetőséget kell biztosítani a küldemény felbontására. Ha egy levélről a felbontást követően derül ki, annak magánjellege, a borítékot vissza kell zárni és a téves felbontás tényéről készült jegyzőkönyvet mellékelve kell átadni az érintett munkavállalónak.

4.11.3 A személyes okmányok másolása

A munkáltató a munkavállalótól olyan nyilatkozat megtételét vagy személyes adat közlését követelheti, amely a munkaviszony létesítése, teljesítése, megszűnése (megszüntetése) vagy az Mt.-ből származó igény érvényesítése szempontjából lényeges. A munkáltató, az üzemi tanács, a szakszervezet jogának gyakorlása vagy kötelességének teljesítése céljából nyilatkozat megtételét vagy adat közlését követelheti. A fentiek alapján az okirat bemutatása követelhető, arról azonban másolat csak törvény vagy uniós rendelet előírása esetén készíthető.

A pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvényben meghatározott kötelezettségek teljesítése érdekében adatkezelő másolatot készít a törvényben meghatározott adatokat tartalmazó bemutatott okiratról, beleértve az okiratban feltüntetett személyes adatokat, azonban a lakcímet igazoló hatósági igazolvány személyi azonosítót igazoló oldala ennek során sem másolható. Egyéb esetekben az általános adatvédelmi rendelet alapján kell megvizsgálni, hogy a másolat elkészítése – megfelelő jogalap megléte esetén – megfelel-e a célhoz kötött adatkezelésnek, valamint a szükségesség-arányosság elvének.

4.11.4 A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően

Az érintett halálát követő öt éven belül az elhaltat életében megillető személyes adatokkal összefüggő jogok érvényesítése az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal meghatalmazott személy jogosult érvényesíteni. Az érintett jogait érvényesítő személy az érintett halálának tényét és idejét halotti anyakönyvi kivonattal vagy bírósági határozattal, valamint saját személyazonosságát közokirattal igazolja. Az adatkezelő kérelemre tájékoztatja az érintett Ptk. szerinti közeli hozzátartozóját a megtett intézkedésekről, kivéve, ha azt az érintett nyilatkozatában megtiltotta. Ilyen jognyilatkozat hiányában az a Ptk. szerinti közeli hozzátartozó jogosult az elhaltat életében megillető jogosultságok érvényesítésére, aki ezen jogosultságát elsőként gyakorolja.

4.11.5 A nyomtatórendszer adatainak kezelése

A Társaság a biztonságos nyomtatás, a munkavégzés hatékonyságának növelése és a költséghatékonyság érdekében központi nyomtatásfelügyeleti rendszert alkalmaz, amely a felhasználók nevét, e-mail címét és AD azonosítóját kezeli, továbbá tárolja az eszköz azonosítóját és

a nyomtatásra, másolásra, illetve szkennelésre vonatkozó adatokat. A rendszer az adatokat egy központi adatbázisban gyűjti, amely biztosítja a jelentések készítését a felügyelt eszközök forgalmáról. Gondoskodni kell arról, hogy a rendszerben tárolt adatokhoz történő hozzáférés csak a szükséges minimális jogosultság elve alapján, naplózott módon történjen.

A felhasználók azonosítása a rendszerben, illetve a multifunkciós eszközökön alapvetően proximity kártyával történik, amely a székházban megegyezik a beléptetéshez használt kártyával. Vendégkártya nyomtatásra történő felhasználása biztonsági okok miatt nem engedélyezett, otthon hagyott beléptető kártya esetén ideiglenesen pin kódos azonosítást kell alkalmazni.

4.11.6 Jelentési és tájékoztatási kötelezettség

Az a munkavállaló, akinek tudomására jut, hogy a Társaság, vagy annak adatfeldolgozója által kezelt személyes adat jogosulatlan személyhez, vagy jogsértő módon került továbbításra, köteles erről a Társaság adatvédelmi tisztviselőjét tájékoztatni, aki intézkedik az eset körülményeinek feltárásáról és – indokolt esetben – az adatkezelő szervezeti egység vezetőjén keresztül gondoskodik az érintett haladéktalan tájékoztatásáról.

4.11.7 A távolról végzett munka / home office

Amennyiben a munkafeladatok ellátása távolról végzett munka útján valósul meg, például home office keretében, és az nem a Társaság által biztosított eszköz igénybevételével történik, a Társaság nem tekinthet be az eszközön tárolt, nem a munkaviszonnyal összefüggő adatokba. Amennyiben a távmunkához a Társaság kizárólag munkavégzés céljára biztosítja az eszközt, a felhasználásával összefüggő tilalom, vagy korlátozás betartásának ellenőrzése céljából a Társaság a teljes adattartalmat ellenőrizheti. A felhasználónak gondoskodnia kell arról, hogy az üzleti titok és más érzékeny adat (pl. személyes adat) ne kerüljön illetéktelen kezekbe. A munkáltató által biztosított eszközöket a Home Office keretében foglalkoztatott munkavállaló köteles rendeltetés szerint használni, azok épségére vigyázni, valamint illetéktelen személyektől távol tartani, azokat kizárólag a Home Office keretében foglalkoztatott munkavállaló használhatja. A munkavállalónak a munkavégzéshez használt informatikai eszközeit és a papír adathordozón lévő adatokat munkaidőn zárható szekrényben kell tárolnia és az otthonról végzett munkavégzés során a személyes adatok kezelésére különös gondot kell fordítania. Az erre a célra használt vállalati eszközön tárolt adatok megfelelő védelméről, a kijelzőn megjelenített adatok bizalmasságáról a felhasználónak minden esetben gondoskodnia kell.

4.11.8 Fénykép- video-, hangfelvétel készítés és felhasználás általános szabályai

Meghatározott személyekről készített fénykép- video-, illetve hangfelvétel személyes adatnak minősül, amelynek elkészítéséhez és felhasználásához az érintett személy hozzájárulása szükséges. A képmás elkészítéséhez történő hozzájárulás a Ptk. alapján ráutaló magatartással is megadható, azonban az általános adatvédelmi rendeletnek megfelelés érdekében célszerű ehhez megfelelő tájékozottságon alapuló írásbeli hozzájárulást is beszerezni. A felvétel felhasználáshoz, nyilvánosságra hozatalához külön hozzájárulás szükséges. A nyilatkozat mintája a 7.8 számú mellékletben megtalálható. Nem szükséges a hozzájárulást beszerezni akkor, amikor a felvétel összhatásában örökít meg nyilvánosság előtt lezajlott eseményeket például tömegfelvétel, illetve nyilvános közéleti szereplés esetén, függetlenül attól, hogy a felvételen az érintett felismerhető-e.

4.11.9 Az értekezleteken készülő hangfelvétel

Az értekezleteken készülő hangfelvétel célja elsősorban a megbeszélésről készített jegyzőkönyv, emlékeztető, határozat pontos elkészítése, illetve szükség esetén a megbeszélésen elhangzottak szöveghű visszaidézése. A hangrögzítés valamennyi érintett hozzájárulásával, illetve – az értekezlet levezetője által adott tájékoztatás ismeretében – kifejezett tiltakozásának hiányában lehetséges. A tájékoztatás elhangzása és a hozzájárulások megadásának dokumentálása történhet a résztvevők jelenlétében a hangrögzítő eszközre történő bemondással, illetve a jelenléti ív aláírásával, az azon szereplő írásos tájékoztató egyidejű elfogadásával, vagy más, az értekezlet rendjét meghatározó szabályzat rendelkezése szerint. Az írásos dokumentum elkészítése során különös figyelemmel kell lenni az adatvédelmi szabályok érvényesítésére. A hangfelvételt, a felhasználásával készített írott dokumentum jóváhagyását, illetve a kezelés indokoltságának megszűnését követően, visszaállíthatatlan módon törölni szükséges. Különösen indokolt esetben – valamennyi érintett kifejezett hozzájárulása esetén – a felvétel csatolható az elkészített emlékeztetőhöz.

4.11.10 Videokonferencia

A videokonferencia felvételének elsődleges célja a megbeszélés kép- és hanganyagának dokumentálása, az arról készített jegyzőkönyv, emlékeztető pontos elkészítése, a megbeszélésen elhangzottak kép- és szöveghű visszaidézése. A felvétel valamennyi érintett tájékozott hozzájárulásával készíthető, illetve kezelhető. A tájékoztatás megtörténtének és a hozzájárulások megadásának dokumentálása történhet a résztvevők jelenlétében a felvételre történő bemondással, illetve a jelenléti ív aláírásával, az azon szereplő írásos tájékoztató egyidejű elfogadásával. A felvételt a felhasználásával készített írott dokumentum jóváhagyását követően, visszaállíthatatlan módon törölni szükséges. Különösen indokolt esetben – valamennyi érintett kifejezett, a jegyzőkönyvben, emlékeztetőben rögzített hozzájárulása esetén – a felvétel csatolható az elkészített emlékeztetőhöz.

4.11.11 Névkitűző viselése

A munkavállaló jogszerűen igazolható cél meghatározása esetén, valamint ha ezen célok más módon nem érhetők el, kötelezhető névkitűző használatára. Ilyen cél lehet például a Társaság objektum vagy területvédelmével összefüggő biztonsági érdeke biztonsági célú kódok jelzések elhelyezésével, illetve munkavállaló ügyfelek által történő megismertetése, azonosításának biztosítása, továbbá az, hogy probléma esetén panasszal élhessenek a munkáltatója felé. A névkitűzőn a munkavállaló fényképe abban az esetben szerepeltethető, amennyiben az érintett ehhez előzetesen hozzájárult, illetve amennyiben a Társaság jogos érdeke ezt alátámasztja és amelyet érdekmérlegelési teszt útján kellőképpen igazolt.

4.11.12 Elektronikus beléptető rendszer alkalmazása

Elektronikus beléptető rendszer az erre vonatkozó megbízási szerződés alapján és akkor alkalmazható, ha jogszabály vagy a terület használatára jogosult rendelkezése szerint a védett területre csak az arra jogosultak léphetnek be. A rendszer működtetése során biztosítani kell az adatvédelmi jogok érvényesülését, valamint szükséges az érintettek tájékoztatása. Az elektronikus beléptető rendszerben a személyes adatok kezelését belső szabályzatban kell rögzíteni, jogos érdek esetén az érdekmérlegelési teszt elkészítésével és a tájékoztatás főbb paramétereinek rögzítésével.

4.11.12.1 Hatósági erkölcsi bizonyítványok kezelése

A munkavállaló vagy a Társasággal munkaviszonyt létesíteni szándékozó személy bűnügyi személyes adata annak vizsgálata céljából kezelhető, hogy a betölteni kívánt vagy a betöltött munkakörben törvény vagy a Társaság nem korlátozza-e vagy nem zárja-e ki a foglalkoztatást. A munkáltató általi korlátozó vagy kizáró feltétel előzetesen és írásban akkor határozható meg, ha az adott munkakörben az érintett személy foglalkoztatása a Társaság jelentős vagyoni érdeke, törvény által védett titka, illetve lőfegyver, lőszer, robbanóanyag őrzéséhez, mérgező vagy veszélyes vegyi vagy biológiai anyagok őrzéséhez, nukleáris anyagok őrzéséhez fűződő törvény által védett jelentős érdeke sérelmének veszélyével járna.

A hatósági erkölcsi bizonyítványhoz kötött munkakörökről szóló EVIG utasításban kell meghatározni a jogszabályi feltételeknek megfelelő munkaköröket, tevékenységeket.

Amennyiben a Társaság az erkölcsi bizonyítványt jelentős vagyoni érdeke, törvény által védett titka, illetve lőfegyver, lőszer, robbanóanyag őrzéséhez, mérgező vagy veszélyes vegyi vagy biológiai anyagok őrzéséhez, nukleáris anyagok őrzéséhez fűződő törvény által védett jelentős érdeke alapján kezeli, abban az esetben érdekmérlegelési teszt elvégzésével kell bemutatni, hogy a Társaság érdeke miként sérülne, ha a foglalkoztatásra az erkölcsi bizonyítvány adata ismeretének hiányában kerülne sor.

A jelentős vagyoni érdek sérelmét megállapító érdekmérlegelési tesztnek tartalmaznia kell a munkakörök és munkaköri feladatok beazonosítását, az erkölcsi bizonyítvány adataihoz kapcsolódás bemutatását, a vagyonelemekkel való kapcsolatot, a kárveszély mértékének beazonosítását, végezetül annak megállapítását, hogy a kárveszély miként tekinthető a Társaság teljes vagyonához viszonyítva jelentősnek.

A pályázókat a meghirdetett munkakör vonatkozásában már az álláshirdetés során tájékoztatni szükséges az adott munkakörben törvény vagy munkáltató általi a foglalkoztatást korlátozó vagy kizáró feltételről és az érintetteket tájékoztatni kell továbbá az adatkezelés főbb elemeiről.

Az erkölcsi bizonyítványt a munkaszerződés megkötését közvetlenül megelőzően kell a munkavállalónak/pályázónak bemutatnia (nem a pályázat benyújtásakor, vagy az elbírálás folyamatában). A bizonyítványról annak online ellenőrzéshez szükséges adatok rögzíthetők, azonban a dokumentumról másolat nem készíthető, a nyilvántartásokban erkölcsi bizonyítvány másolata nem kezelhető. Az erkölcsi bizonyítvány tartalmának rendszeres időközönként (pl. évente) történő ellenőrzését elnök-vezérigazgatói utasítás elrendelheti, amennyiben az előzetesen meghatározott munkakörök esetében indokolt (pl. gépjárművezető estében a foglakoztatástól való eltiltás).

4.11.12.2 Összeférhetetlenségi nyilatkozat
Az összeférhetetlenség kezeléséről külön normatív EVIG utasításban kell rendelkezni. A Társasággal történő munkaszerződés megkötésekor, a foglalkoztatási viszonyaiban, vagy az összeférhetetlenségi nyilatkozat tartalmában történt változásokat megelőzően tett összeférhetetlenségi nyilatkozatot zártan kell kezelni.

4.11.13 A személyes adatokat tartalmazó iratok, adathordozók kezelése
A személyes adatokat tartalmazó iratok, adathordozók kizárólag zárt borítékban (vagy egyéb, ezzel egyenértékű megoldással, pl. számkódos táska) továbbíthatók és azokon fel kell tüntetni a „Zártan kezelendő!" kezelési jelölést. Ezt a megjelölést a személyes adatok elektronikus adattovábbítása, valamint elektronikus megjelenítése során is alkalmazni kell. Kivételt képeznek azok az elektronikus adattovábbítások, melyek tartalmi és formai elemeit jogszabály, vagy jogszabály felhatalmazása alapján a felügyeleti hatóság írja elő, valamint a Humán szolgáltatás belső szervezeti egységei közötti adattovábbítás, amennyiben megfelelően biztosított a munkavállalói személyes adatok illetéktelen hozzáférés elleni védelme. Az így jelölt adattartalom esetében gondoskodni kell az adatok védett kezeléséről oly módon, hogy azokhoz kizárólag a megismerési jogosultsággal rendelkezők, dokumentált módon férhessenek hozzá – elektronikus feldolgozás, továbbítás esetén, a rendelkezésre álló lehetőségek felhasználásával – technikai védelemmel (pl. a társaság által rendszeresített titkosítási módszerrel) is biztosítani kell. A kezelési jelölést a dokumentumon és a személyes adatok feldolgozására használt alkalmazások segítségével a számítógépek monitorán is meg kell jeleníteni. Az adatok az érintett életében csak akkor hozhatók nyilvánosságra, ha azt törvény elrendeli, vagy ahhoz az érintett hozzájárult.

4.11.14 Gyermekek adatainak hozzájárulás alapján történő kezelése
A 14 év alatti cselekvőképtelen kiskorú – például gyermekvasutas – nevében a törvényes képviselője jár el. A 14 és 18 év közötti korlátozottan cselekvőképes kiskorú jognyilatkozatának érvényességéhez a törvényes képviselőjének hozzájárulása szükséges. A 16. életévét betöltött gyermek kizárólag az információs társadalommal összefüggő, közvetlenül gyermekeknek kínált szolgáltatások vonatkozásában önállóan adhat hozzájárulást. A gyermekeket is megilletik az érintetti jogok, amelyeket az általános adatvédelmi rendelet meghatároz (az érintett törléshez való joga különösen fontos olyan esetekben, amikor még gyermekként adta meg az adatkezeléshez a hozzájárulást).
Az olyan esetekben, amikor az adatkezelést végző szervezeti egység még szülői beleegyezéshez kötött hozzájárulás alapján kezeli az adatokat, nyomon kell, hogy kövesse, hogy az érintett gyermek mikor éri el azt a kort, amikor önállóan is megadhatja a hozzájárulását és ekkor ezt a megerősítést be is kell szereznie tőlük.

4.11.15 Üzemi tanács, üzemi megbízott, munkavédelmi képviselő választás adatkezelése
Az Mt. alapján az üzemi tanács jogának gyakorlása vagy kötelességének teljesítése céljából jogszerűen kezeli a választásra jogosult, valamint a választható munkavállalók névsorát, amelyet a választási bizottság állapít meg és a választást megelőzően legalább ötven nappal közzéteszi. Az ehhez szükséges adatokat a választási bizottság kérésére, a munkáltató öt napon belül adja meg. A munkavédelmi képviselő, illetve az illetve az üzemi megbízott választásra is az üzemi tanács választására vonatkozó szabályokat kell alkalmazni. A választással összefüggő adatkezelés szabályainak kialakítása során fokozottan ügyelni kell az adatvédelmi előírásokra, különösen a

személyes adatok különleges kategóriáinak (érdekképviseleti tagság) kezelésére, az adatminimalizálásra, átláthatóságra vonatkozó előírásokra, valamint a célhoz kötött adatkezelésre.

4.11.16 Megkeresés alapján történő adattovábbítás

A Társasághoz külső szervezettől, illetve magánszemélytől érkező, a MÁV Zrt. közzétételi szabályzatáról szóló utasítás hatálya alá nem tartozó, személyes adat kiadására irányuló megkeresés csak akkor teljesíthető, ha az érintett erre írásban felhatalmazza a Társaságot. Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra és a megkereséssel élő szervek meghatározott körére.

Az adatközlést az érintett nyilatkozattételétől függetlenül teljesíteni kell, ha azt jogszabály írja elő, így különösen büntető ügyekben eljáró hatóságoktól – rendőrség, bíróság, ügyészség, TEK, NAV stb. – valamint a nemzetbiztonsági szolgálatoktól érkező megkereséseket. E szervezetek megkereséseiről, amennyiben ennek egyéb törvényi akadálya nincs – az elrendelt nemzetbiztonsági ellenőrzések lefolytatása során történő iratbetekintések, adatkérések kivételével – az illetékes adatkezelést végző munkavállaló közvetlenül, vagy felettese útján köteles a jegyzőkönyv megküldésével tájékoztatni biztonsági főigazgatót, akinek jóváhagyását követően kell az adatszolgáltatást a meghatározott határidőn belül teljesíteni. A főigazgató a nemzetbiztonsági szolgálatok adatkérésre irányuló megkeresése ellen nem halasztó hatályú panasszal fordulhat az illetékes miniszterhez. A nemzetbiztonsági szolgálatoktól érkező megkeresés alapján teljesített adatszolgáltatásról, adatbetekintés biztosításáról, illetve a Társaság nyilvántartásban történő jelzés elhelyezésére vonatkozó tényről, azok tartalmáról, valamint a megtett intézkedésekről az érintett, illetőleg más személy, vagy szervezet nem tájékoztatható.

4.11.17 Közbeszerzések

A közbeszerzések során is figyelemmel kell lenni a beépített és az alapértelmezett adatvédelem elveinek megfelelő érvényesítésére, azaz a természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme teljesítését biztosító technikai és szervezési intézkedések meghozatalára. A Társaságnak a megfelelés igazolása érdekében is, olyan belső szabályokat kell meghoznia és alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik a beépített és az alapértelmezett adatvédelem elveit. A személyes adatok kezelésén alapuló vagy rendeltetésük teljesítéséhez személyes adatokat kezelő termékek, szolgáltatások és alkalmazások beszerzésekor a szállítókat arra kell ösztönözni, hogy szem előtt tartsák a személyes adatok védeleméhez való jogot, és a tudomány és technológia állását kellően figyelembe véve gondoskodjanak arról, hogy az adatkezelő és az adatfeldolgozó adatvédelmi kötelezettségeinek eleget tegyen.

4.11.18 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 adatmentesítési eljárások). Mobiltelefon esetében például a készülék alaphelyzetbe történő visszaállításról, a memóriakártya adatmentesítéséről, a SIM kártya eltávolításáról és megsemmisítéséről, notebook esetében a felhasználói profilok, azok tartalmával együtt és a vállalati adatoknak (pl. levelezés, mappák) a törléséről. Ezen szabályok szerint kell eljárni az elektronikus adathordozót tartalmazó talált tárgyak értékesítése esetén is.

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

A Társaság munkavállalójának személyes adatát EGT-n kívüli országba csak az általános adatvédelmi rendelet által meghatározott feltételekkel, az érintett tevékeny, kizárólag erre a célra irányuló hozzájárulása esetén továbbíthat, amennyiben az adatkezelés során megfelelő szinten biztosított a továbbított személyes adatok védelme. Ebbe a körbe tartoznak az IBSZ által meghatározott felhő alapú rendszerekben kezelt személyes adatok is, amennyiben egyértelműen nem határozható meg az adatok tárolási helye.

4.11.20 Személyes adatkezelést megvalósító kamerás térfigyelő rendszerek alkalmazása

4.11.21 Kamerakezelés az Szsztv. alapján

A Társaságnál működtetett elektronikus személyes adatkezelést megvalósító megfigyelőrendszer működési feltételeit alapvetően az Szsztv. 8. §, valamint 8/A §-ai határozzák meg. Az Szsztv. meghatározza azon szolgáltatók és adatkezelési célok körét, amelyek közérdekből, kötelező adatkezelési jogcímen képfelvételt készíthetnek és ezen adatok körét kezelik. A felvételeket készítő rendszerek üzemeltetését, mint adatkezelést a belső adatkezelési nyilvántartásba be kell jelenteni.

A Társaság, mint személyszállítási közszolgáltatást végző szolgáltató, illetve vasútállomás, megállóhely üzemeltetője e szolgáltatással összefüggésben a járműveinek, a területén található berendezéseknek, eszközöknek, az utasoknak, valamint a szolgáltató munkavállalói és megbízottai életének, személyének, testi épségének és a nemzeti vagyon védelme céljából elektronikus biztonságtechnikai rendszeren keresztül az alábbi feltételekkel folytathat megfigyelést, készíthet rögzített képfelvételt és kezelheti a rögzített képfelvételeket.

Képfelvétel a Társaság a tulajdonában vagy jogszerű használatában álló területen, a közforgalom számára nyitva álló helyen, a vasúti pályahálózaton, személyszállítási szolgáltatás céljára alkalmazott járművein, valamint a jegy- és bérletértékesítő berendezéseken készíthető. Nem készíthető felvétel olyan helyen, ahol az az emberi méltóságot sértheti (pl. mosdóban, illemhelyen). A személyes adatok kezeléséről a vasútállomás és megállóhely, illetve a Társaság tulajdonában vagy jogszerű használatában álló terület bejáratánál, a személyszállító vasúti járműre való felszállásra szolgáló peronoknál, a jegy- és bérletértékesítő berendezések környezetében tájékoztatást, továbbá a kamerák látószögében figyelemfelhívó jelzést (piktogram) kell elhelyezni a 7.3 számú mellékletben szereplő minta szerint. A Vagyonvédelmi utasítás szerint korábban kihelyezésre került piktogramokat fokozatosan kell lecserélni a jelen utasításban szereplő szöveges változatra. Ezeket elsősorban az újonnan létesítésre kerülő kamerarendszereknél kell kihelyezni, illetve gondoskodni kell a korábbi figyelemfelhívó jelzések fokozatos lecseréléséről. Amennyiben a tájékoztatás elhelyezésére a hely sajátosságai miatt nincs mód (pl. műemlék épület), akkor a tájékoztatást a Társaság honlapján kell hozzáférhetővé tenni. A tájékoztatást a vakok és gyengén látók, valamint idegen nyelvűek számára is értelmezhető módon (pl. hangosbemondó útján, idegen nyelven) kell megtenni.

A felvételt a rögzítéstől számított 15 napig kell megőrizni és a 16. napon törölni kell. Akinek jogát vagy jogos érdekét a képfelvétel érinti, kérheti, hogy a felvételen szereplő adatok kezelését annak kezelője korlátozza (ne törölje). A bíróság vagy hatóság megkeresés esetén a felvételt haladéktalanul meg kell küldeni részükre. Abban az esetben, ha a kérelem benyújtásától számított 30 napon belül bíróság vagy hatóság részéről megkeresés nem érkezik, a felvételt törölni kell.

A felvétek a Társaság szolgáltatását igénybe vevő személyeket, a működtetésben lévő berendezések használóit, a Társaság munkavállalóit, megbízottjait, a Társaság kezelésében lévő területeken tartózkodó személyeket, illetve poggyászaikat, és a járműveket, berendezéseket és felszereléseket ért balesetek, káresetek körülményeinek, továbbá a panaszbejelentések kivizsgálásához használhatók fel.

Vizsgálat esetén, annak időtartamával, de legfeljebb 45 nappal a bekezdésben meghatározott 15 napos megőrzési idő meghosszabbítható. A felvételeket a vizsgálat és az annak eredményeként tett intézkedések, illetve bírósági vagy hatósági eljárás esetén az azt lezáró határozat jogerőre emelkedését vagy véglegessé válását követő 15. napon törölni kell.

A tárolás vagy a hozzáférés is adatkezelésnek minősül, ezért az adatkezelőnek és/vagy adatfeldolgozó-nak biztosítania kell a felvételek bizalmasságát és sértetlenségét. Az élőképet csak az arra feljogosított személyek (pl. vagyonőr) tekinthetik meg. A rögzített felvételeket a központi minta alapján elkészített helyi adatkezelési szabályzatban meghatározott feladatkört betöltő személyek, valamint a felvételhez betekintési, illetve hozzáférési jogával élő személyek nézhetik vissza. Az érintett esetében a felvételen esetlegesen szereplő további személyek képét ki kell takarni. A felvételek titkosságát és integritását biztosítani kell, például elektronikus formátumban titkosítva és

fizikai formátumban elzárva történő tárolás útján. A felvételekhez történő hozzáféréseket és az adattovábbításokat dokumentálni szükséges.

A kamerakezeléssel összefüggő adatkezelési tájékoztató rövid, illetve teljes szövegének mintája a 7.3 és a 7.4 számú mellékletben található.

Adatfeldolgozó igénybe vétele esetén adatfeldolgozói szerződést, vagy megállapodást kell kötni, amelyben egyértelműen meghatározásra kerülnek szerepek és a hatáskörök, mind az adatkezelő az adatfeldolgozó, mind az ügyfél esetében. Ennek vázlata a 7.11 számú mellékletben szerepel.

4.11.22 Kamerakezelés az Fbőtv. előírásainak megfelelően

A fegyveres biztonsági őr elektronikus megfigyelőrendszer működtetése (a továbbiakban: megfigyelőrendszer) útján kép-, hang-, valamint kép- és hangfelvételt (a továbbiakban: felvétel) a fegyveres biztonsági őrzésből adódó kötelezettségei teljesítése érdekében,

a) a létesítmény telephelyének védelme,
b) a radioaktív és veszélyes anyagok őrzése,
c) a rendkívüli események megelőzése, következményeinek elhárítása, kivizsgálásának segítése,
d) a jogsértések észlelése,
e) az elkövető tettenérése, valamint
f) a jogsértő cselekmények megelőzése

céljából, az általános adatvédelmi rendelet szerinti adatvédelmi jogok érvényesítése mellett készíthet, illetve kezelhet, amely tevékenysége során adatkezelőnek minősül.

A fegyveres biztonsági őr megfigyelőrendszert a védett létesítmény területe és annak környezete megfigyelésére alkalmazhat.

A felvételt felhasználás hiányában a közterületet is érintő felvétel esetén a rögzítéstől számított három nap, egyéb esetben hatvan nap elteltével meg kell semmisíteni, illetve törölni kell.

A felvétel, vagy az abban szereplő személyes adat felhasználható

a) a rögzítés helyszínén elkövetett bűncselekmény, szabálysértés miatt indult büntető-, szabálysértési vagy más hatósági eljárás során,
b) körözött személy vagy tárgy azonosítása vagy intézkedés jogszerűségének közigazgatási eljárásban történő vizsgálata céljából,
c) az érintett személy jogainak gyakorlása érdekében.

Az, akinek jogát vagy jogos érdekét a felvétel, vagy abban szereplő személyes adatának rögzítése érinti, a meghatározott időtartamon belül kérheti, hogy a felvételt, vagy abban szereplő személyes adatot kezelője ne semmisítse meg, illetve ne törölje. A nyomozó hatóság, a szabálysértési hatóság, az ügyészség, a bíróság, a nemzetbiztonsági szolgálatok, nemzetközi jogsegély keretében külföldi hatóság a meghatározott időtartamon belül kezdeményezheti, hogy a felvételt, vagy abban szereplő személyes adatot kezelője ne semmisítse meg, illetve ne törölje.

A felvételt – a jogszabályban meghatározott szabálysértési, bűnüldözési, igazságszolgáltatási, valamint nemzetbiztonsági célból – a nyomozó hatóság, a szabálysértési hatóság, az ügyészség, a bíróság, a nemzetbiztonsági szolgálatok, nemzetközi jogsegély keretében külföldi hatóság, jogainak gyakorlása érdekében az érintett, valamint a jogszabály alapján eljárás kezdeményezésére irányuló jogának gyakorlása érdekében harmadik személy részére lehet átadni.

Ha a felvétel felhasználására sor került, akkor a határidő lejártát követően haladéktalanul meg kell semmisíteni, illetve törölni kell.

A közterületet is érintő megfigyelőrendszerrel védett terület esetén a védelemre kötelezett szervezet vezetője jól látható helyen, jól olvashatóan, a területen megjelenni kívánó harmadik személyek tájékozódását elősegítő módon köteles figyelmeztető jelzést elhelyeztetni

a) a területre bevinni tilos tárgyakról, azok jellegéről;
b) arról a tényről, hogy az adott területen megfigyelőrendszert alkalmaznak;
c) a megfigyelőrendszer által folytatott megfigyelés, valamint a rendszer által rögzített, személyes adatokat tartalmazó felvétel 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 általános adatvédelmi rendeletnek az érintettek jogaira és érvényesítésük rendjére vonatkozó rendelkezéseiről; valamint
d) a fegyveres biztonsági őr intézkedései által okozott jogsérelem esetén igénybe vehető eljárásokról.

Nem alkalmazható a létesítményt figyelő megfigyelőrendszer olyan helyen, ahol a megfigyelés az emberi méltóságot sértheti, így különösen öltözőben, orvosi rendelőben, mosdóban és fürdőben, illemhelyen.

Az adatkezelőnek biztosítania kell, hogy az érintett személy személyes adatai, magántitkai, és a magánéletére vonatkozó egyéb adatok, tények ne jussanak illetéktelen személy tudomására.

4.11.23 Másolat kérése kamerás adatkezelés esetén

Az érintettek – bármely jogalap alapján történő kamerás adatkezelés esetén – élhetnek azzal a jogukkal, hogy másolatot kérjenek minden olyan felvételről, amelyen szerepelnek. Az adatkezelőnek egy hónap áll rendelkezésére a kérés teljesítéshez (amely egy alkalommal, legfeljebb két hónappal meghosszabbítható). Biztosítani kell azonban, hogy a kiadásra kerülő felvételen csak az érintett szerepeljen, és annak kiadásával ne kerüljön nyilvánosságra semmilyen más adatalany személyes adata (pl. képmása, cselekedete). Ez szükségessé teheti az arcok, mozgások vagy rendszámtáblák stb. felismerhetetlenné tételét is. A felvételek másolatát díjmentesen kell biztosítani az érintett számára. Ha a kérelem egyértelműen megalapozatlan vagy különösen ismétlődő jellege miatt, túlzó, az adatkezelő – figyelemmel az adminisztratív költségekre – észszerű összegű díjat számíthat fel, illetve kellő indok mellett meg is tagadhatja a kérelem teljesítését. Kamerafelvétel kikérése esetén fel kell hívni az adatigénylő figyelemét arra, hogy a felvételek adatkezelésének korlátozása szükségtelenné teszi a felvételen szereplő egyéb személyek kitakarását, egyúttal a beavatkozásmentes felvétel bemutatásának pl. a hatóság, bíróság előtt nagyobb bizonyító ereje lehet. A személyes adat kiadására vonatkozó kérelem mintáját a 7.10 számú melléklet tartalmazza.

4.11.24 Személyes adatkezelést nélkülöző kamerák alkalmazása

4.11.24.1 Technológiai kamerák

A technológiai kamerák konkrét eszközök (pl. utastájékoztató tábla) megfigyelésére irányulnak, illetve használatukkal oly módon figyelhető meg valamely terület, hogy látókörében személyek felismerhető módon nem fordulhatnak elő, illetőleg természetes személy nem válik azonosíthatóvá a felvételen szereplő bármely információ alapján, így személyes adatkezelés nem valósul meg. A technológiai kamerákra az általános adatvédelmi rendelet rendelkezései ez esetben nem vonatkoznak, de a környezetében megjelenő személyek tájékoztatása céljából a kamera jelenlétére utaló jelzést ki kell helyezni. Amennyiben a technológiai célból telepített térfigyelő eszközök látóterében akár alkalmi jelleggel is előfordul azonosított vagy azonosítható természetes személy megjelenése, abban az esetben a személyes adatok kezelésére vonatkozó valamennyi előírást megfelelő módon érvényesíteni szükséges.

4.11.24.2 A személyes jelenlétet helyettesítő videokamerás megfigyelő rendszerek

A kép és hangrögzítés nélküli, személyes jelenlétet helyettesítő videokamerás megfigyelő rendszerek alkalmazásakor azonos módon kell a személyes adatok kezelését dokumentálni és elvégezni, mint ahogy az a rögzítő berendezéssel ellátott megfigyelő rendszerek esetében szükséges.

4.11.25 Elektronikus beléptető rendszer alkalmazása

Az Szvmt. alapján elektronikus beléptető rendszer az erre vonatkozó megbízási szerződés alapján és akkor alkalmazható, ha jogszabály vagy a terület használatára jogosult rendelkezése szerint a védett területre csak az arra jogosultak léphetnek be. Az adatkezelő jogos érdeke alapján határozza meg az adatkezelési időtartamot. A bárki számára nyitott területen nem alkalmazható elektronikus beléptető rendszer. A beléptető rendszerek kapcsán az érintettek megfelelő tájékoztatása nem maradhat el.

4.11.26 Ügyfélszolgálat igénybevétele során történő adatkezelés

Ügyfélszolgálathoz beérkező valamennyi telefonon tett szóbeli panaszt, valamint az ügyfélszolgálat és a felhasználó közötti telefonos kommunikációt hangfelvétellel rögzíteni kell. A hangfelvételt egyedi azonosítószámmal kell ellátni, öt évig meg kell őrizni, és a felhasználó kérésére, díjmentesen rendelkezésre kell bocsátani. A hangfelvétel készítésével, megőrzésével és rendelkezésre bocsátásával kapcsolatos kötelezettségről, továbbá az egyedi azonosítószámról a felhasználót a telefonos ügyintézés kezdetekor tájékoztatni szükséges. A Társaságnál működtetett telefonos ügyfélszolgálat esetén, e szabályok érvényesítésén túl, az általános adatkezelési szabályoknak is meg kell felelni, így többek között el kell készíteni az adatkezelési szabályzatot, továbbá közzé kell tenni az adatkezelési tájékoztatót.

4.11.27 A Társaság honlapja

A Társaság honlapján lehetőség van hírlevél szolgáltatás igénybevételére, vagy más értesítésre történő feliratkozásra, véleménykérő lap működtetésére, amely során név, cégnév és elérhetőségi adatok (e-mail cím, telefonszám stb.) kerülnek rögzítésre. A regisztrációs adatok kizárólag a szolgáltatással kapcsolatosan használhatóak fel, harmadik fél részére nem adhatók át. A szolgáltatás felmondására minden esetben lehetőséget kell biztosítani, amely során a korábban felvett adatokat visszaállíthatatlanul törölni kell. A honlapon hivatkozást kell elhelyezni, amely tartalmazza a honlap adatkezelésére vonatkozó Adatkezelési tájékoztatót és adatvédelmi nyilatkozatot. A honlapon korábban elhelyezett nyilatkozatokat a honlap tartalmáért felelős szervezetnek naprakészen kell tartania. Az utolsó változat aktualizálásának időpontját fel kell tüntetni. A szabályozásban bekövetkezett változásról a hírlevélre feliratkozottakat tájékoztatni szükséges.

4.11.28 A Társaság honlapját látogatók számítógépén cookie elhelyezéséről

Az Eht. szabályozza a cookie (a továbbiakban: süti) használatát, amely alapján a felhasználó elektronikus hírközlő végberendezésén csak az érintett világos és teljes körű – az adatkezelés céljára is kiterjedő – tájékoztatását követő kifejezett hozzájárulása alapján lehet adatot tárolni, vagy az ott tárolt adathoz hozzáférni. A felhasználót adatvédelmi tájékoztató útján előzetesen teljes körűen és részletesen tájékoztatni kell a számítógépére felmásolni kívánt adatokról, majd miután ehhez megfelelően dokumentált hozzájárulását adta, tölthető fel a süti az eszközére. A süti elhelyezőjének bizonyítani kell tudnia, hogy a felhasználó a hozzájárulását megadta. A Társaság honlapján a sütik kezelését e szabályoknak megfelelően kell kialakítani, és azokat az adatkezelési nyilatkozat megfelelően dokumentált elfogadását követően lehet a felhasználó végberendezésén elhelyezni.

4.11.29 Az idegen személyek magáncélú fényképfelvétel készítése a Társaság üzemi területén

A MÁV Zrt. üzemi területén történő tartózkodás rendjéről külön normatív utasítás rendelkezik. A magáncélú fényképfelvétel készítési engedély kiadásához szükséges regisztráció során az engedélyt kiállító szervezet a kérelmező személyi adatait nyilvántartásban rögzíti, amely alapján a kérelmező regisztrációs igazolványt kap. A személyes adatok kezelésének szabályait helyi adatkezelési szabályzatban szükséges rögzíteni, amelynek lényeges elemeit az érintettek számára közérthető módon megfogalmazott adatvédelmi tájékoztatóban elérhetővé kell tenni.

4.11.30 Drón felhasználásával megvalósított adatkezelés

A drónokkal, illetve az azokra szerelhető kiegészítőkkel (pl. kamera, mikrofon) megvalósuló adatkezelés még az eszköz rendeltetésszerű használata esetén is rendkívül erős behatolást jelenthet a személyek a magánszférájába, ezért a Társaság adatkezelést megvalósító drónt kizárólag az alábbi feltételekkel használhat, illetve ilyen eszköz használatát az alábbi feltételek szerint teheti lehetővé.

A Társaság területén drón használatának engedélyezésére az ezen eszközök alkalmazására vonatkozó jogszabályokban, illetve belső utasításokban meghatározott engedélyek birtokában kerülhet sor.

Amennyiben a drónnal készített kép- és hangfelvételek elkészítése során személyek azonosítására alkalmas felvételek rögzítésére kerül sor, vizsgálni szükséges – többek között – a kérelmező által meghatározott célt, a jogalapot, az alkalmazás szükségességét és arányosságát, a tájékoztatási kötelezettség teljesítését, valamint az adatkezelés törvényességi feltételeinek teljesülését. Meg kell követelni az adatvédelmi előírások betartását, valamint a Ptk. fényképkészítésre és a személyiségi jogokra vonatkozó előírásainak érvényesülését.

Az adatkezelés megkezdése nem csupán a Társaság engedélyéhez kötött, hanem eseti légtér kijelölése iránti kérelemmel be kell szerezni az érintett légügyi hatóság erre irányuló engedélyét is. Tekintettel a drón speciális jellegére különös gondossággal kell eljárni a megfelelő tájékoztatáson alapuló hozzájárulás beszerzése érdekében. Biztosítani kell az érintett számára, hogy a drón használatával megvalósított adatkezelés ellen tiltakozhasson, ennek során az adatkezelés megszüntetését, illetve a kezelt adatok törlését kérje.

A drónok vasúti technológiai, ingatlankezelési, kommunikációs, illetve vagyonvédelmi célú alkalmazása során, munkavállalók azonosítására alkalmas felvételek készítése esetén, *a munkavállaló ellenőrzése* című fejezetben meghatározott követelményeket is teljesíteni kell.

A Társaság területének meghatározása során az idegen személyek MÁV Zrt. területén történő tartózkodásának, magáncélú fényképfelvétel készítésének, engedélyezésének, a külső vállalkozók MÁV Zrt. területén történő munkavégzésének munkavédelmi feltételeiről és engedélyezésének rendjéről szóló normatív utasításban meghatározottak az irányadók.

4.11.31 Előterjesztések, szabályzatok készítése

Amennyiben a Társaság belső előterjesztésében, illetve szabályzatának tervezetében személyes adatkezelés azonosítható és az a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal jár, a jogszabályi rendelkezéseknek való megfelelést külön ki kell emelni és az adatkezelőnek az adatkezelést megelőzően hatásvizsgálatot kell végeznie arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Ennek érdekében a 4.8.5 pontban meghatározott Adatvédelmi hatásvizsgálat szerint kell eljárni.

4.11.32 Közérdekből nyilvános személyes adatok

Az Infotv. előírásai szerint a Társaságnak lehetővé kell tennie, hogy az általa kezelt közérdekből nyilvános személyes adatokat – egyedi igénylés alapján – bárki megismerhesse, illetve a kötelezően közzéteendő adatokat az internetes honlapján elérhetővé tegye. Közérdekből nyilvános személyes adat a Társaság feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízása, a közfeladat ellátásával összefüggő egyéb személyes adata, valamint azok a személyes adatai, amelyek megismerhetőségét törvény előírja. A Társaság feladat- és hatáskörében eljáró munkavállalói kört az SZMSZ I. kötete állapítja meg. A MÁV Zrt. közzétételi szabályzata biztosítja a hozzáférést a közérdekű és közérdekből nyilvános adatok megismerésére irányuló igények esetén, illetve előírja a Társaság tevékenységével kapcsolatos legfontosabb közérdekű adatokra vonatkozóan a közvélemény elektronikus tájékoztatását. Közérdekű illetve közérdekből nyilvános adat megismerése iránti igényt bárki benyújthat a Társaság felé. A kért adatot az igénybeérkezését követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül kell az igénylő részére kiadni, illetve megküldeni. Amennyiben az igényelt adat nem megismerhető adatot is tartalmaz, azt a kiadást megelőzően felismerhetetlenné kell tenni. Az adatigénylő személyes adatai csak az igény teljesítéséhez, illetve annak teljesítéséért megállapított költségtérítés megfizetéséhez szükséges mértékben és ideig kezelhetők, amelyet követően az igénylő személyes adatait haladéktalanul törölni kell.
Amennyiben az adatigénylés azonos igénylő által egy éven belül benyújtott, azonos adatkörre irányuló adatigényléssel megegyezik, és az azonos adatkörbe tartozó adatokban változás nem állt be, az adatigénylésnek az adatot kezelő közfeladatot ellátó szerv nem köteles eleget tenni. Ennek érdekében az adatigénylések, valamit az adatkezelők adatait egy évig meg kell őrizni.

5.0 HIVATKOZÁSOK, MÓDOSITÁSOK, HATÁLYON KÍVŰL HELYEZÉSEK

Hivatkozások

- A MÁV Zrt. és a jelen utasításban felsorolt leányvállalatok válságkezelési és válságkommunikációs feladatairól szóló 76/2017. (XI. 17. MÁV Ért. 28.) EVIG utasítás.
- A MÁV Zrt. védendő információi biztonsága érdekében bevezetett adatszivárgást megelőző (DLP) rendszer működtetésének feltételeiről szóló 63/2017. (IX. 01. MÁV Ért. 23.) EVIG utasítás
- Az internet hozzáférés biztosításának és használatának szabályairól szóló 90/2017. (XII. 22. MÁV Ért. 32.) EVIG utasítás

A szabályzat által nem érintett közérdekből nyilvános személyes adatok kezelésével kapcsolatos kérdésekben

- a MÁV Zrt. közérdekű adatai megismerésére irányuló igények teljesítésének rendjéről és az elektronikus közzététel szabályairól szóló 7/2017. (I. 20. MÁV Ért. 3.) EVIG sz. utasítás (Közzétételi szabályzat),
- informatikai biztonsági és ügyviteli kérdésekben a MÁV Zrt. Informatikai Biztonsági Szabályzatáról szóló hatályos EVIG utasítás, illetve
- a hatályos ügyviteli-iratkezelési szabályzatok előírásai szerint kell eljárni.

Hatályon kívül helyezés
Ezen szabályzat hatálybalépésével egyidejűleg hatályát veszti a MÁV Zrt. Adatvédelmi Szabályzatáról szóló 39/2015. (MÁV. Ért. 17.) EVIG. sz. utasítás.

6.0 HATÁLYBA LÉPTETŐ RENDELKEZÉS

A szabályzat a közzétételt követő 15. napon lép hatályba és visszavonásig érvényes. A szervezeti egységek vezetői gondoskodjanak arról, hogy munkavállalóik a szabályzatban szabályozott – tevékenységükhöz kapcsolódó – ismereteket elsajátítsák. A jelen szabályzatban foglalt előírásoknak történő megfelelés érdekében az adatkezelést végző szervezeti egységek vezetői gondoskodjanak az irányításuk alá tartozó adatkezelők felé az adatkezelések áttekintésére.

7.0 MELLÉKLETEK JEGYZÉKE

Az utasítás mellékletei az utasítás módosítása, újbóli kiadása nélkül is aktualizálhatók, kiegészíthetők, a karbantartásért felelős szervezeti egység által. Az utasítás mellékletei csak elektronikusan kerülnek közzétételre. Az utasítás hatályos mellékletei a Társaság utasítástárában érhetők el.

7.01 A személyes adatokat tartalmazó dokumentumok álnevesítése, anonimizálása
7.02 Adatvédelmi tájékoztató és nyilatkozat a kommunikációs eszközök használatáról
7.03 Adatkezelési tájékoztató a MÁV Zrt. területén üzemeltetett térfigyelő rendszerről (rövid)
7.04 Adatkezelési tájékoztató a MÁV Zrt. területén üzemeltetett térfigyelő rendszerről (teljes)
7.05 Adatkezelés bejelentése a MÁV Zrt. adatkezelési nyilvántartásába
7.06 Az adatfeldolgozói megállapodás – vázlat
7.07 Nyilatkozat az informatikai eszközök adattartalmáról az eszköz visszaszolgáltatásakor
7.08 Nyilatkozat az érintett önkéntes hozzájárulása alapján történő fénykép-, video-, hangfelvétel
elkészítéséhez és felhasználásához
7.09 Jegyzőkönyv a MÁV Zrt.-hez érkező személyes adatokat érintő adatkérésről és adatszolgáltatásról
7.10 Személyes adat kiadására vonatkozó kérelem
7.11 Érdekmérlegelési teszt minta
7.12 Kérdőív az adatvédelmi hatásvizsgálathoz
7.13 Az adatkezelés kialakításának folyamatábrája

dr. Homolya Róbert s.k.
elnök-vezérigazgató