Készítette: MÁV Személyszállítási Zrt.
Szervezeti egység: Megfelelés támogatás

8/2025. (I. 01.) sz.
vezérigazgatói utasítás

az Adatvédelmi Szabályzatról

……
Dr. Mosóczi László
vezérigazgató

Tartalomjegyzék

1.0 AZ UTASÍTÁS CÉLJA

Az utasítás célja, hogy a vonatkozó adatvédelmi jogszabályok tükrében meghatározza a MÁV Személyszállítási Zrt. (a továbbiakban: Társaság) által a személyes adatokon végzett adatkezelések – függetlenül attól, hogy a Társaság az adatkezelések során adatkezelőként vagy adatfeldolgozóként jár el – adatvédelmi megfelelőségének biztosításához szükséges általános keretszabályokat. A Társaság egyes feladatai, ezáltal az adatkezelési folyamatai tekintetében kiadott szabályozásokban a jelen utasításban foglaltak figyelembevételével, a tevékenységspecifikus adatkezelési rendelkezések meghatározása szükséges.

2.0 HATÁLY ÉS FELELŐSSÉG MEGHATÁROZÁSA

2.1 Az utasítás hatálya

2.1.1 Az utasítás személyi hatálya

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

2.1.2 Az utasítás tárgyi hatálya

Az utasítás tárgyi hatálya kiterjed a Társaság szervezeti egységeinél, vagy a Társasággal szerződéses jogviszonyban álló adatfeldolgozóknál folytatott minden olyan adatkezelésre, amely személyes adatra vonatkozik, függetlenül attól, hogy az adatkezelés teljesen vagy részben automatizált eszközzel, vagy manuálisan történik.

Ha a Társaság adatfeldolgozóként végez adatkezelést, úgy a jelen utasítást a Társaság és az adatkezelő között létrejött adatfeldolgozási szerződés rendelkezéseinek figyelembevételével és annak elsődlegességével kell alkalmazni.

2.1.3. Az utasítás időbeli hatálya

Az utasítás előírásait, annak személyi és szervezeti hatálya alá tartozók a hatálybalépés időpontjától, annak hatályon kívül helyezéséig kötelesek betartani és végrehajtani.

2.2 Az utasítás kidolgozásáért és karbantartásáért felelős, az utasításban előírtak betartatásáért felelős

Az utasítás elkészítéséért és szükség szerinti aktualizálásáért a Társaság Megfelelés támogatás szervezet vezetője és az Adatvédelmi tisztviselő közösen felel. Az utasításban előírtak betartatásáért a feladatkörében minden adatkezelő szervezeti egység vezetője felelős.

3.0 FOGALMAK MEGHATÁROZÁSA

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.

Adatkezelési folyamat: az adatkezelő szervezeti egység egy konkrét feladatával összefüggésben, a személyes adatokon egy meghatározott adatkezelési célból végzett adatkezelési művelet vagy műveletek összessége.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajttatja.

Adatkezelő szervezeti egység: a Társaság mindenkor hatályos Szervezeti és Működési Szabályzata szerinti szervezeti egysége, amely az adatkezelést a Társaság nevében és érdekében végzi.

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki, vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – az adatkezelő nevében személyes adatokat kezel, adatfeldolgozást végez.

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

Az adatvédelmi munkacsoport: a Társaság adatkezelő szervezeti egységeinek – munkáltatói jogkörgyakorlója által kijelölt – munkavállalóiból álló, az adatvédelmi tisztviselő által irányított csoport.

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

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

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

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

Adatvédelmi felügyeleti hatóság vagy Hatóság: a nemzeti jog által kijelölt illetékes adatvédelmi felügyeleti hatóság. A jelen utasítás kiadásakor az adatvédelmi felügyeleti hatóság feladatait a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH vagy adatvédelmi hatóság) látja el.

Adatvédelmi jogszabály: a jelen utasítás alkalmazása körében adatvédelmi jogszabálynak minősül az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR), az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), az adatkezelési folyamat tekintetében irányadó szakági jogszabályok, valamint az Európai Adatvédelmi Testület iránymutatásai, továbbá a NAIH állásfoglalásai, iránymutatásai, ajánlásai és döntései.

Adatvédelmi szakértő(k): az adatvédelmi tisztviselő közvetlen irányítása alatt álló szakértő(k), aki(k) segíti(k) az adatvédelmi tisztviselő munkáját.

Adattovábbítás: az adat meghatározott harmadik fél számára történő hozzáférhetővé tétele (rendelkezésre bocsátása).

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

Adatvédelmi kockázatelemzés és hatásvizsgálat: az adatkezelés előzetes kontrollja a kockázatok feltárása és a kockázatok mérséklésére teendő intézkedések értékelése érdekében.

Adatvédelmi tisztviselő (Data Protection Officer, DPO): a Társaság által a GDPR-ban, valamint a jelen utasításban foglalt adatvédelmi megfelelőségi feladatok ellátására kijelölt – a NAIH részére bejelentett – személy.

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

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.

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 (pl. ujj- és tenyérlenyomat).

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. Az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően alkalmazandó adatvédelmi szabályoknak.

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

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

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

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

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

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

Kockázat: a jelen utasítás értelmezésében olyan tény, körülmény vagy esemény (ideértve a mulasztást is), amely az adatkezelési folyamatban nem megfelelőséget eredményezhet.

Kockázatkezelés: az adatkezelési folyamatot érintő kockázat(ok) kezelésére hozott intézkedések összessége.

Közös adatkezelő: két vagy több adatkezelő, akik közösen határozzák meg az adatkezelés céljait és eszközeit, illetve közösen hozzák meg az adatkezelésre vonatkozó döntéseket, hajtják végre azokat, vagy hajtatják végre azokat az adatfeldolgozókkal.

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

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik.

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 kategóriája: 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.

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

3.1 Kulcsszavak

3.1.1 A szabályozás tartalmára utaló kulcsszavak: adatvédelem, GDPR, személyes adat, érintett, adatvédelmi incidens, adatkezelés

3.1.2 A szervezeti egységre vonatkozó kulcsszavak: megfelelés, adatvédelem, adatvédelmi tisztviselő

4.0 AZ UTASÍTÁS LEÍRÁSA

4.1. A személyes adatok kezelésének általános szabályai

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

Amennyiben a Társaság önálló adatkezelőként jár el, úgy az adatkezelések jogszerűségéért harmadik személyek irányában a Társaság a felelős. Amennyiben a Társaság más adatkezelő adatfeldolgozójaként jár el, úgy az adatkezelés jogszerűségéért harmadik személyek irányában – az adatfeldolgozási szerződés rendelkezéseinek figyelembevételével – az adatkezelő felelős. Az adatkezelő és az adatfeldolgozó közötti felelősség telepítésére vonatkozó rendelkezéseket az adatfeldolgozási szerződésben kell rögzíteni. Amennyiben a Társaság adatfeldolgozóként végez adatkezelést, de a személyes adatok kezelésének célját – az adatkezelő utasításaival ellentétesen – önállóan határozza meg, túlterjeszkedik az adatfeldolgozási szerződésben foglalt jogain, úgy harmadik személyek irányában az adott túlterjeszkedéssel érintett adatok tekintetében önálló adatkezelőként felel.

A Társaság, mint adatkezelő, köteles olyan adatfeldolgozókat igénybe venni, akik/amelyek megfelelő garanciákat nyújtanak az adatkezelés GDPR-ban foglalt követelményeinek való megfelelésre és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

A Társaság irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező munkavállalók által végzett adatkezelést a Társaság által végzett adatkezelésnek kell tekinteni. A munkavégzésük során személyes adatok kezelését végző munkavállalókat – ideértve más foglalkoztatásra irányuló jogviszony keretében foglalkoztatott személyeket is – titoktartási kötelezettség terheli, amelyről a munkaviszony, illetve egyéb szerződéses jogviszony létesítésekor titoktartási nyilatkozatot kötelesek tenni.

A titoktartás keretében a személyes adat nem hozható nyilvánosságra és azok kezelésére nem jogosult harmadik személy rendelkezésére nem bocsátható, kivéve, ha a személyes adat közérdekből nyilvános adatként történő nyilvánosságra hozatalát, vagy rendelkezésre bocsátását jogszabály írja elő. A Társaság munkavállalói kötelesek megtenni azokat az ésszerű intézkedéseket, amelyek kizárják annak a lehetőségét, hogy a szóban elhangzott, papíralapon vagy elektronikus formátumban rögzített személyes adatot harmadik személy jogosulatlanul megismerje.

Személyes adatról papíralapú vagy elektronikus másolat csak abban az esetben készíthető, ha azt az adatkezelés folyamata szükségessé teszi, vagy azt jogszabály előírja.

A Társaság munkavállalói munkajogi, polgári jogi és büntetőjogi felelősséggel tartoznak a munkájuk során végzett adatkezelési műveletek jogszerűségéért és a jelen utasításban foglaltak betartásáért.

A jelen utasításban foglaltakat a mindenkor hatályos Informatikai Biztonsági Szabályzattal (a továbbiakban: IBSZ) összhangban kell alkalmazni.

4.2. Az adatkezeléssel összefüggő feladatok, hatáskörök és felelősség

4.2.1. A Társaság vezérigazgatója

a) Meghatározza, illetve jóváhagyja a Társaság adatkezeléssel járó tevékenységeinek adatvédelmi követelményeit.
b) Jelen utasítás keretei között:
   ba) Meghatározza az adatvédelem szervezeti rendszerét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket.
   bb) Biztosítja a Társaság által végzett adatkezelések jogszerűségének feltételeit.
   bc) Gyakorolja az adatvédelmi megfelelőségi vizsgálattal kapcsolatos jelen utasításban foglalt jogokat.

4.2.2. Adatkezelő szervezeti egység vezetője

a) Gondoskodik a jelen utasításban foglalt, az adatkezelő szervezeti egységeket terhelő kötelezettségek betartásáról, amelyért az adatkezelő szervezeti egység felelősséggel tartozik.
b) Kijelöli az adatkezelő szervezeti egységet képviselő adatvédelmi munkacsoport tagját és biztosítja, hogy a munkacsoport tagja részt vegyen az adatvédelmi munkacsoport ülésein.
c) Biztosítja az adatkezelő szervezeti egység által végzett adatkezelés tekintetében az adatvédelmi felügyeleti hatóság által indított eljárásban a vizsgálat lefolytatásához szükséges feltételeket, és együttműködik az adatvédelmi felügyeleti hatóság által feltett kérdések megválaszolásában és információk szolgáltatásában.
d) Biztosítja az adatkezelő szervezeti egység valamely adatkezelési folyamata tekintetében végzett adatvédelmi megfelelőségi vizsgálat lefolytatásához szükséges információt és együttműködik a vizsgálat teljeskörű lefolytatásában, valamint biztosítja az adatvédelmi megfelelőségi vizsgálat eredményének végrehajtását.

e) Amennyiben az adatkezelő szervezeti egység által végzett valamely adatkezelési folyamat tekintetében a Társaság közös adatkezelőnek minősül, úgy gondoskodik a GDPR 26. cikk (1) bekezdés szerinti és annak megfelelő közös adatkezelésre vonatkozó megállapodás megkötéséről.
f) Amennyiben az adatkezelő szervezeti egység valamely adatkezelési folyamata keretében adatfeldolgozót vesz igénybe, úgy gondoskodik a GDPR 28. cikk (3) bekezdés szerinti és annak megfelelő adatfeldolgozási szerződés előkészítéséről és megkötéséről.

4.2.3. Megfelelés támogatás szervezet vezetője

a) Az adatvédelmi tisztviselővel közösen gondoskodik az Adatvédelmi Szabályzat elkészítéséről, szükség szerinti felülvizsgálatáról és aktualizálásáról.
b) Javaslatot tesz a vezérigazgató részére az adatvédelmi tisztviselő személyére.
c) Biztosítja az adatvédelmi tisztviselő feladatainak ellátásához és szakmai ismereteinek fenntartásához szükséges feltételeket.

4.2.4. Adatvédelmi tisztviselő

Az adatvédelmi tisztviselő a Társaságban az alábbi feladatokat látja el:

a) Tájékoztat és szakmai tanácsot ad a Társaság bármely munkavállalója részére az adatvédelmi jogszabályoknak való megfelelés érdekében.
b) Hivatalból vagy bármely munkavállaló kérésére hivatalos állásfoglalást bocsát ki valamely adatkezelési folyamat adatvédelmi jogszabályoknak való megfelelőségéről. Az adatvédelmi tisztviselő hivatalból akkor bocsát ki állásfoglalást, ha
   ba) az adatkezelési folyamat nagyszámú személyes adatot vagy érintetti kört érint,
   bb) az adatkezelési folyamat keretében a személyes adatok különleges kategóriájába tartozó adatok kezelésére is sor kerül,
   bc) az adatkezelési folyamat magas kockázatú adatkezelésnek minősül.
c) A jelen utasításban foglaltak szerint az éves auditálási terv szerint, illetve hivatalból vagy megbízólevél alapján lefolytatja az adatvédelmi megfelelőségi vizsgálatot, amely során ellenőrzi az egyes adatkezelési folyamatok adatvédelmi jogszabályoknak való megfelelését.
d) Minden tárgyév december 15. napjáig jóváhagyásra előterjeszti a Társaság vezérigazgatója részére a következő évre vonatkozó adatvédelmi auditálási tervet.
e) Közreműködik a Társaság adatvédelmi oktatásával kapcsolatos feladatok ellátásában.
f) Közreműködik a részére bejelentett adatvédelmi incidensek kivizsgálásában, és szakmai tanácsot ad az incidens következményeinek elhárításához szükséges intézkedések meghatározásához, továbbá – amennyiben a GDPR és a jelen utasításban foglaltak szerint annak feltételei fennállnak – az adatvédelmi incidens bekövetkezését bejelenti az adatvédelmi felügyeleti hatóságnak és az adatkezelő szervezeti egység által adott információk alapján kialakítja szakmai álláspontját arról, hogy szükség van-e az érintettek értesítésére.
g) Gondoskodik a Társaság honlapján található adatvédelmi menüpont naprakészen tartásáról, ennek keretében gondoskodik az egyes adatkezelési tájékoztatók honlapon való közzétételéről, valamint biztosítja az adatvédelmi menüpont tartalmának adatvédelmi jogszabályoknak való megfelelését.
h) Ellátja az adatvédelmi munkacsoport működésével összefüggő feladatokat.
i) Figyelemmel kíséri a hazai és a nemzetközi adatvédelmi gyakorlatot, ideértve az egyes európai adatvédelmi hatóságok angol nyelven is elérhető döntéseit és az Európai Unió Bírósága által hozott adatvédelmet érintő döntéseket, amelyek alapján a Társaság tekintetében is releváns – adekvátan alkalmazható – döntésekről tájékoztatást nyújt a döntésben foglalt gyakorlattal érintett szervezet(ek) részére.
j) A Társaság nevében kapcsolatot tart és együttműködik az adatvédelmi felügyeleti hatósággal.
k) Vezeti a társasági szintű adatkezelési tevékenységek nyilvántartását és a részére bejelentett adatvédelmi incidenseket tartalmazó nyilvántartást.

l) Minden tárgyév január 31. napjáig írásban éves jelentést készít a tárgyévet megelőző év Társaságot érintő legfontosabb adatvédelmi kérdéseiről, amelyet megküld a Társaság vezérigazgatója részére.
m) Ellátja a jelen utasításban foglalt, az adatvédelmi tisztviselőre delegált egyéb feladatokat.

Az adatvédelmi tisztviselő feladatai ellátása során jogosult betekinteni a Társaságnál végzett adatkezelésekkel kapcsolatos dokumentumokba, informatikai rendszerekbe, szükség szerint azokról másolatot kérhet, jogosult továbbá felvilágosítást és tájékoztatást kérni a Társaság bármely munkavállalójától.

Az adatvédelmi tisztviselő jogállására a GDPR 38. cikkét kell alkalmazni azzal, hogy feladatait a Megfelelés támogatás szervezet keretében látja el. Az adatvédelmi tisztviselő akadályoztatása esetén elsődlegesen a feladatok ellátásáért a Megfelelés támogatás szervezet vezetője felelős, illetve az adatvédelmi tisztviselő helyettesítéséről a Megfelelés támogatás szervezet vezetője gondoskodik a helyettes kijelölése útján.

4.2.5. Biztonsági Főigazgatóság információvédelmi szakterülete

a) Közreműködik a személyes adatokkal kapcsolatos valamennyi olyan adatbiztonsági feladat ellátásában, amely tekintetében a mindenkor hatályos IBSZ rendelkezéseit alkalmazni kell.
b) Közreműködik a Társaságnál bekövetkezett, információvédelmi érintettségű adatvédelmi incidensek kivizsgálásában.

4.2.6. A Társaság honlapjának szerkesztéséért felelős szervezet vezetője

Közreműködik az adatvédelmi tisztviselőnek a Társaság honlapjával kapcsolatos feladatai teljesítésében.

4.2.7. Adatvédelmi munkacsoport

4.2.7.1. Az adatvédelmi munkacsoport tagjai

Az adatvédelmi munkacsoport tagja az adatvédelmi tisztviselő és az adatkezelő szervezeti egységek munkáltatói jogkörgyakorlója által írásban – ideértve az elektronikus utat is – kijelölt munkavállalók. A munkáltatói jogkörgyakorlók a munkacsoport tagjait az adatkezelő szervezeti egység feladatait jól ismerő munkavállalók közül – az adatvédelmi tisztviselő felhívására – jelölik ki. Az adatkezelő szervezeti egység adatkezelési folyamatainak számára és összetettségére tekintettel több munkacsoport tag is kijelölhető. Amennyiben indokolt, az adatvédelmi tisztviselő javaslatot tehet az adatkezelő szervezeti egység munkáltatói jogkörgyakorlója részére további munkacsoport tag kijelölésére.

Amennyiben a munkáltatói jogkörgyakorlója az adatvédelmi munkacsoportba nem kíván munkacsoport tagot kijelölni, azt – a munkacsoport tag kijelölésére vonatkozó felhívásra adott írásbeli válaszában – indokolnia kell. A munkacsoport tag kijelölésének mellőzéséről és annak indokáról az adatvédelmi tisztviselő tájékoztatja a Megfelelés támogatás szervezet vezetőjét.

A munkacsoport tagság bármely okból történő megszűnése, valamint új szervezeti egység létesítése esetén az adatvédelmi tisztviselő – a munkacsoport tagság megszűnését, valamint a szervezeti egység létesítését követő – 15 napon belül írásban tájékoztatja a munkáltatói jogkör gyakorlót a munkacsoport tag kijelölésének szükségességéről.

4.2.7.2. Az adatvédelmi munkacsoport működése, hatásköre és feladatai

Az adatvédelmi munkacsoport az adatvédelmi tisztviselő koordinálásával az adatkezelő szervezeti egységek adatvédelmi megfelelését segíti elő. Az adatvédelmi tisztviselő az adatvédelmi munkacsoport ülésein az adatvédelmi tudatosság növelését és az adatvédelmi megfelelőség segítését célzó oktatást tart.

Az adatvédelmi munkacsoport tagja továbbá,

- részt vesz az adatvédelmi munkacsoport ülésén, távolmaradása esetén azt jelzi az adatvédelmi tisztviselő részére,
- közreműködik az adatkezelő szervezeti egységnél bevezetésre kerülő új adatkezelési folyamat kockázatelemzésében, valamint a folyamatban lévő adatkezelési folyamatok kockázatelemzésének kialakításában és felülvizsgálatában, amelybe bevonja az adatvédelmi tisztviselőt,
- közreműködik a hatásvizsgálattal érintett adatkezelési folyamatok esetén a hatásvizsgálat elvégzésében és szükség esetén az előzetes konzultációban,
- tájékoztatja az adatvédelmi tisztviselőt az adatkezelő szervezeti egységnél bevezetni tervezett új adatkezelési folyamatról, illetve annak tervezési szakaszába bevonja,
- közreműködik az adatkezelő szervezeti egység adatkezelési tevékenysége nyilvántartásának naprakészen tartásában, amelynek keretében késedelem nélkül, de legfeljebb 5 munkanapon belül bejelenti az adatvédelmi tisztviselő részére az adatkezelő szervezeti egység új adatkezelési folyamatát, valamint az adatkezelési tevékenységek nyilvántartásában szereplő adatkezelési folyamatok változása esetén szolgáltatja a változással érintett információkat,
- közreműködik az őt foglalkoztató adatkezelő szervezeti egység valamely adatkezelési folyamatára irányuló adatvédelmi megfelelőségi vizsgálat lefolytatásában,
- adatvédelmi incidens esetén részt vesz az incidens kivizsgálásában, a szükséges dokumentumok létrehozásában, kitöltésében,
- tájékoztatja az adatvédelmi tisztviselőt és a munkáltatói jogkörgyakorlóját az adatkezelő szervezeti egységben bekövetkezett és tudomására jutott adatvédelmi incidens gyanús esetekről, illetve azok körülményeiről,
- a NAIH megkeresése esetén részt vesz a megkeresésben érintett adatkezelési folyamattal kapcsolatos tények kiderítésében, az információk összegyűjtésében és a választervezet elkészítésében,
- információszolgáltatás útján közreműködik az adatvédelmi tisztviselő által a jelen utasítás szerint kiadott állásfoglalás előkészítésében,
- közreműködik az adatkezelő szervezeti egység adatkezelési folyamatainak adatvédelmi megfelelőségéhez szükséges dokumentumok, így különösen az adatkezelési tájékoztatók, érdekmérlegelési tesztek elkészítésében,
- tájékoztatja az adatvédelmi tisztviselőt az adatkezelő szervezeti egység adatkezelési folyamatait érintő tényekről,
- közreműködik az olyan érintetti kérelmek megválaszolásához szükséges információk megszerzésében és a választervezet előkészítésében, amely az általa képviselt adatkezelő szervezeti egység valamely adatkezelési folyamata tekintetében érkezett a Társasághoz,
- ellátja a jelen szabályzat vagy más, a Társaság utasításában megfogalmazott adatkezeléssel kapcsolatos feladatokat.

Az adatvédelmi munkacsoport munkáját az adatvédelmi tisztviselő koordinálja, ideértve az adatvédelmi munkacsoport üléseinek összehívását, az ülések levezetését, az ülések dokumentálását, valamint az adatvédelmi munkacsoport tagok feladatainak végrehajtásában való közreműködést is.

Az adatvédelmi munkacsoport évente legalább két alkalommal ülést tart. Az adatvédelmi tisztviselő az adatvédelmi munkacsoport feladatairól és az adatvédelmi munkacsoport üléseinek tervezett időpontjáról éves feladattervet készít, amelyet az adatvédelmi munkacsoport első ülésén ismertet a munkacsoport tagjaival.

Az adatvédelmi munkacsoport üléséről jegyzőkönyvet kell készíteni, amelyet a tárgyévet követő 5 évig az adatvédelmi tisztviselő őriz meg. A jegyzőkönyvnek tartalmaznia kell az ülés időpontját, az ülésen részt vevő személyek listáját (név és szervezeti egység), az ülésen történt események leírását, az ülésen elhangzott nyilatkozatok – szükség esetén szó szerinti – leiratát, valamint más, az ülés dokumentálása szempontjából lényeges információt.

Az adatvédelmi munkacsoport működésével összefüggő dokumentumokat a Társaság közös meghajtóján erre a célra létrehozott közös mappában (a továbbiakban a jelen pont keretében: „mappa") kell tárolni. A mappa létrehozásáért és naprakészen tartásáért az adatvédelmi tisztviselő felelős. A mappához az adatvédelmi munkacsoport tagjai – a jelen utasításban foglalt kivétellel – kizárólag olvasási jogosultsággal rendelkezhet.

Az adatvédelmi munkacsoport működése során végzett adatkezeléssel összefüggő adatkezelési tájékoztató elkészítéséért az adatvédelmi tisztviselő felelős. Az adatkezelési tájékoztatót az adatvédelmi munkacsoport tag részére a kijelölést követően küldött tájékoztató levélben közölni kell, valamint azt folyamatosan elérhetővé kell tenni az adatvédelmi munkacsoport mappájában.

4.3. A személyes adatok kezelésének alapelvei

A személyes adatok kezelésének minden szakaszában – az adatkezelési folyamat tervezésétől annak befejezéséig – érvényesülnie kell, az alábbi alapelveknek.

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

b) A célhoz kötöttség elvének megfelelően a Társaság személyes adatot csak meghatározott, jogszerű célból, jog gyakorlása vagy kötelezettség teljesítése érdekében kezelhet, a cél eléréséhez szükséges mértékben és ideig.

Eredeti céltól eltérő célból adatkezelés akkor végezhető, ha az eltérő célú adatkezelés összeegyeztethető azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték és az eltérő célú adatkezeléshez az érintett hozzájárult vagy az valamely – a GDPR 23. cikk (1) bekezdésben foglalt korlátozásokkal kapcsolatos uniós vagy tagállami jogon alapul. Ha az eltérő célból végzett adatkezelés jogszerűsége nem az előzőekben felsorolt jogalapok valamelyikén alapul, úgy annak – dokumentált módon történő – vizsgálata során, hogy az eltérő célú adatkezelés összeegyeztethető-e az eredeti céllal a GDPR 6. cikk (4) bekezdés a) – e) pontjaiban foglalt körülményeket szükséges figyelembe venni.

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

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

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

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

f) Az integritás és bizalmas jelleg elvének és a beépített és alapértelmezett adatvédelem elvének megfelelően az adatkezelést úgy kell kialakítani, hogy megfelelő technikai és/vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága. Gondoskodni kell a személyes adatok jogosulatlan vagy jogellenes kezelésének – ideértve a személyes adatokhoz való jogosulatlan hozzáférést is – megakadályozásáról, illetve biztosítani kell a véletlen elvesztés, megsemmisítés vagy károsodás elleni védelmet.
Ennek biztosítása érdekében a Társaság az egyes adatkezelési folyamataira vonatkozó szabályozás keretében az adatkezelés kockázatainak figyelembevételével meghatározza azokat a technikai és/vagy szervezési intézkedéseket, amelyekkel a személyes adatok integritása és bizalmassága biztosítható.

g) Az elszámoltathatóság elvének való megfelelés keretében a Társaságra hárul annak a felelőssége, hogy bizonyítsa az a) – f) pontban megjelölt alapelveknek való megfelelést. Az egyes adatkezelési folyamatok adatvédelmi megfelelőségének igazolásához – az elszámoltathatóság elvének való megfeleléshez – szükséges intézkedéseket az egyes adatkezelési folyamatokat szabályozó belső utasításokban kell meghatározni.

4.4. A személyes adatok kezelésének jogalapja és feltétele

A Társaságnál személyes adat jogszerűen csak akkor kezelhető, ha a GDPR 6. cikk (1) bekezdésében foglalt valamely jogalap fennáll. A személyes adatok különleges kategóriájába tartozó személyes adat jogszerűen abban az esetben kezelhető, ha a GDPR 6. cikk (1) bekezdésben foglalt valamely jogalap fennállása mellett a GDPR 9. cikk (2) bekezdésében foglalt valamely további feltétel fennáll. Az adatkezelés jogalapjának meghatározása során az adatvédelmi jogszabályokban foglaltakon túl a jelen utasítás rendelkezéseit szükséges figyelembe venni. Egy adatkezelés folyamat keretében egy adatkezelési célból végzett adatkezelés jogszerűségét egy jogalap biztosíthatja. Amennyiben egy személyes adat kezelése több adatkezelési célból történik, úgy az adatkezelés jogszerűségét biztosító jogalapot célonként kell meghatározni és ennek megfelelően több adatkezelési folyamat indul.

4.4.1. A személyes adatok kezelésének jogalapja

a) Az érintett (kifejezett) hozzájárulása

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

Az elszámoltathatóság elvéből következően, ha az adatkezelés hozzájáruláson alapul, az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult. Ezért a hozzájárulásnak dokumentáltnak, és visszakereshetőnek kell lennie.
Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja, amely más ügyekre is vonatkozik, az egyes hozzájáruló nyilatkozatokat egyértelműen el kell különíteni egymástól.

Az Adatkezelőnek az érintett hozzájárulását adatkezelési célonként kell beszereznie. Ha egy adatkezelés több olyan célból történik, amelynek jogszerűségét az érintett hozzájárulása biztosítja, úgy az Adatkezelőnek olyan formában kell beszereznie a hozzájáruló nyilatkozatot, hogy az érintett, célonként külön-külön tudja megadni hozzájárulását.

Amennyiben a hozzájáruló nyilatkozat nem felel meg a GDPR és a jelen utasítás rendelkezéseinek, úgy a hozzájáruló nyilatkozat érvénytelen és az adatkezelés jogszerűtlen.

Az érintett hozzájárulását bármikor visszavonhatja, a hozzájárulás visszavonására a Társaságnak olyan egyszerű megoldást kell biztosítania, mint amilyen egyszerűen megadhatta az érintett a hozzájárulását. A hozzájárulás visszavonása nem érinti a visszavonás előtti adatkezelés jogszerűségét, erről az érintettet a hozzájárulást megelőzően tájékoztatni kell.

A közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában hozzájárulás alapján végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A nem információs társadalommal összefüggő szolgáltatások esetén a 16. életévét betöltött kiskorú gyermek,– mint érintett – hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása szükséges, kivéve, ha a hozzájáruló nyilatkozat olyan adatkezeléssel függ össze, amely tekintetében a 16. életévét betöltött kiskorú gyermek a vonatkozó jogszabályoknak megfelelően tehet önálló jognyilatkozatot. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezeléséhez törvényes képviselő hozzájárulása szükséges. Az adatkezelési folyamatot e szabálynak megfelelően kell kialakítani.

b) Szerződés teljesítése

Az adatkezelés 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 elsősorban az Adatkezelő és a Társaság utasai vagy természetes személy üzleti partnerei között létrejött, illetve a Társaság munkavállalójával kötött szerződés teljesítése keretében megvalósuló, vagy ahhoz kapcsolódó személyes adatok kezelése esetén alkalmazandó.

c) Jogi kötelezettség teljesítése

Az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. Ezt az adatkezelő elsősorban akkor alkalmazhatja, ha a személyes adatok kezelését jogszabály kifejezetten előírja. E jogalap alapján végzett adatkezelést hatályos uniós- vagy tagállami jognak kell megállapítania.

d) Az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme

Az adatkezelés az érintett vagy másik természetes személy létfontosságú érdekeinek védelmében történik, különösen, ha az adatkezelés az érintett életét, testi épségét, egészségét vagy személyek vagyonát fenyegető közvetlenül fennálló veszély, körülmény elhárításához szükséges.

e) Közérdekű feladat végrehajtása

Az adatkezelés akkor jogszerű, ha az jogszabály által meghatározott közérdekű feladat (közfeladat) végrehajtásához szükséges. Amennyiben a közérdekű feladatot meghatározó jogszabály nem felel meg az Infotv. 5.§ (3) bekezdésben foglaltaknak, úgy az adatkezelés szükségességét a Társaságnak igazolnia kell. E jogalap alapján végzett adatkezelést hatályos uniós- vagy tagállami jognak kell megállapítania.

f) Jogos érdek érvényesítése

Az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekének érvényesítéséhez szükséges. A jogos érdek, mint jogalap alkalmazása csak akkor lehetséges, ha az adatkezelő vagy harmadik fél jogos érdekei elsőbbséget élveznek az érintett érdekeivel vagy alapvető jogaival és szabadságaival szemben, amelyek személyes adatok védelmét teszik szükségessé. Az adatkezelő szervezeti egység a jogos érdek alátámasztása érdekében – az adatvédelmi tisztviselő szakmai közreműködése mellett – a jelen utasításban foglaltak szerint köteles érdekmérlegelési tesztet elvégezni. A jogos érdek jogalapja akkor áll fenn, ha az érdekmérlegelési teszt eredményeként az adatkezelő szervezeti egység arra a következtetésre jut, hogy az adatkezelő vagy egy harmadik fél jogos érdekei elsőbbséget élveznek az érintett érdekeivel, alapvető jogaival és szabadságaival szemben.

4.4.2. A személyes adatok különleges kategóriáiba tartozó személyes adatok kezelésének további feltételei

A 4.4.1. pontban foglaltaknak megfelelően igazolt jogalap fennállásán túl a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, 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 kezelése a Társaságnál kizárólag akkor lehetséges, ha

- az érintett kifejezett hozzájárulását adta az említett személyes adatok kezeléséhez, és azt jogszabály kifejezetten nem tiltja,
- a foglalkoztatást, szociális biztonságot és védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges,
- az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, és az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni,
- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott,
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges,
- az adatkezelés jelentős közérdek miatt szükséges, megfelelő garanciákat biztosító jogszabályi háttér megléte esetén,
- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges,
- az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan,
- az adatkezelés a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő,
- a Társaságnál bűnügyi személyes adat kizárólag abban az esetben kezelhető, ha azt az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó uniós vagy tagállami jog lehetővé teszi.

4.5. Érintetti jogok és azok gyakorlására irányuló kérelem teljesítése

A Társaságnak a személyes adatok kezelésének teljes szakaszában biztosítania kell az érintetti jogok gyakorlásának lehetőségét. Az érintetti jogok gyakorlását – az adathordozhatósághoz való jog kivételével – attól függetlenül kell biztosítani, hogy az adatkezelés automatizált vagy nem automatizált módon történik. Az érintetti jogok gyakorlására irányuló kérelmek elbírálási folyamatába az adatvédelmi tisztviselő bevonása kötelező.

4.5.1. Az érintettet megillető jogok

Az egyes érintetti jogok gyakorlására való jogosultság az alábbiak szerint függ az adatkezelés jogalapjától:

- a hozzájárulás visszavonásához való jog csak abban az esetben illeti meg az érintettet, ha az adatkezelés jogalapja az érintett hozzájárulása;
- a tiltakozáshoz való jog gyakorlása csak abban az esetben illeti meg az érintettet, ha az adatkezelés jogszerűségét a közérdekű feladat végrehajtása vagy a jogos érdek jogalapok egyike biztosítja;
- az adathordozhatósághoz való jog abban az esetben gyakorolható, ha az adatkezelés jogalapja az érintett hozzájárulása vagy a szerződéses jogalap és az adathordozhatósághoz való jog további feltételei is fennállnak.

Az érintettet megillető jogok gyakorolhatóságáról szóló áttekintést a 8. számú függelék tartalmazza.

a) Előzetes tájékoztatáshoz való jog

Amennyiben az adatkezelő szervezeti egység a személyes adatokat az érintettől szerzi meg, az adatkezelésre vonatkozó tájékoztatási kötelezettségének a GDPR 13. cikke szerint (adatkezelési tájékoztató minta az 1. számú függelék alatt) – az ott megjelölt tartalommal – az adatkezelés megkezdését megelőzően köteles eleget tenni. Amennyiben az adatkezelő szervezeti egység a személyes adatokat nem az érintettől szerzi meg, az adatkezelésre vonatkozó tájékoztatási kötelezettségének a GDPR 14. cikke szerint – az ott megjelölt tartalommal – az adatkezelési tájékoztató minta (mely az 1. számú függelékben képezi) megfelelő módosításával köteles eleget tenni. Az adatkezelő szervezeti egység a tájékoztatást a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül; ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor köteles teljesíteni. A Társaság nem köteles tájékoztatni az érintettet, ha az érintett személyes adatait nem az érintettől szerzi meg és a tájékoztatás teljesítése lehetetlennek bizonyul, aránytalanul nagy erőfeszítést igényelne, vagy valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné az adatkezelés céljainak elérését.

Az előzetes tájékoztatáshoz való jog tekintetében a 4.6.3.3. pont rendelkezéseit kell alkalmazni.

b) Hozzáféréshez való jog

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e. A hozzáférés joga alapján az érintett jogosult tájékoztatást kérni a személyes adatainak kezelésére vonatkozó információkról [ba) pont], jogosult másolatot kérni a Társaság által kezelt személyes adatairól [bb) pont], valamint jogosult a személyes adataiba betekinteni [bc) pont].

ba) Tájékoztatáshoz való jog

Az érintett kérelmére a Társaság tájékoztatást ad az általa kezelt adatokról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatkezelő nevéről, címéről (székhelyéről), az adatfeldolgozók

nevéről, címéről (székhelyéről) és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi tisztviselő elérhetőségéről, továbbá – amennyiben az adatkezelési folyamatban adattovábbítás történt vagy történik – az adattovábbítás címzettjéről, illetve az adattovábbítás céljáról, továbbá az érintettet az adatkezeléssel összefüggő jogairól és a joggyakorlás módjáról.

A tájékoztatáshoz való jog gyakorlására irányuló kérelem nem teljesíthető az adatkezelésre irányadó adatkezelési tájékoztató érintett részére történő megküldésével.

bb) Másolatkéréshez való jog

A Társaság az érintettre vonatkozó személyes adatok másolatát az érintett rendelkezésére bocsátja. A másolatot az érintett kérelmétől függően, papír alapon, elektronikus dokumentumban vagy digitális adathordozón kell rendelkezésre bocsátani.

A személyes adatok másolatának érintett részére történő megküldése elektronikus formában kizárólag az érintett által megjelölt e-mail címre történő megküldéssel történhet, amelyhez jelszóval ellátott mellékletben kell csatolni a személyes adatok másolatát tartalmazó elektronikus dokumentumot. A titkosítás feloldásához szükséges jelszóról az érintettet biztonságos, az elektronikus levelezéstől eltérő csatornán kell tájékoztatni. Amennyiben az érintett tájékoztatásához az elektronikus levelezéstől eltérő csatorna nem vehető igénybe, úgy az érintettet a személyes adatok másolatát tartalmazó elektronikus levéltől eltérő levélben kell tájékoztatni a titkosítás feloldásához szükséges jelszóról, vagy a jelszó meghatározásának feltételeiről. Az érintett személyes adatait tartalmazó dokumentumot nem szükséges hitelesíteni. Az érintett által az adott személyes adatról első alkalommal kért másolat ingyenes, azonban minden további másolatért észszerű mértékig a Társaság költségtérítést állapíthat meg. A költségtérítés megállapítása érdekében az adatkezelő szervezeti egység az adatvédelmi tisztviselő közreműködésével egyeztet a Gazdasági Főigazgatósággal.

A másolatkéréshez való jog teljesítése nem érintheti hátrányosan mások jogait és szabadságait, ezért a személyes adatok másolata kizárólag úgy bocsátható az érintett rendelkezésére, hogy más személyre vonatkozó személyes adatokat törölni, illetve anonimizálni kell.

bc) Betekintéshez való jog

Az érintett a betekintéshez való jog gyakorlása esetén jogosult arra, hogy a Társaság által kezelt, személyes adatait tartalmazó nyilvántartásokba vagy más, a személyes adatait tartalmazó felvételbe, dokumentumba betekintsen. A betekintési jog gyakorlása során a betekintéssel érintett dokumentumokról papír alapú vagy elektronikus másolat – ideértve a fényképfelvételt is – nem készíthető. A betekintési jog gyakorlását az adatkezelő szervezeti egység biztosítja, amelyen az adatvédelmi tisztviselőnek – amennyiben ez nem lehetséges az érintett adatkezelő szervezeti egységet képviselő adatvédelmi munkacsoport tagnak – részt kell vennie. Az adatvédelmi tisztviselő akadályoztatása esetén a Megfelelés támogatás vezető gondoskodik olyan személy kijelöléséről, aki feladatköre szerint jogosult adatvédelmi kérdésekben eljárni.

Amennyiben a betekintési jogot a Társaság munkavállalója gyakorolja a munkaviszonyával összefüggésben keletkezett személyes adatot tartalmazó dokumentumok tekintetében, úgy a betekintési jog gyakorlását a területileg illetékes humánpartner, illetve akadályoztatása esetén a dokumentum kezelésére jogosult szakértő biztosítja.

A betekintési jog gyakorlásáról – más normatív szabályozó kifejezett eltérő rendelkezés hiányában - a 10. számú függelék szerinti jegyzőkönyvet kell felvenni. A jegyzőkönyvet a betekintési jog gyakorlását biztosító és annak gyakorlása során jelen lévő munkavállaló(k)nak és a betekintési jogot gyakorló érintettnek vagy az érintett képviseletében eljáró személynek alá kell írnia. Amennyiben az érintett, vagy az érintett képviseletében eljáró személy a jegyzőkönyv aláírását megtagadja, úgy ennek tényét a jegyzőkönyvben rögzíteni kell. A jegyzőkönyvet két példányban kell felvenni,

amelyből egy példány az érintettet és egy példány az adatkezelő szervezeti egységet illet azzal, hogy a jegyzőkönyv megőrzését az adatvédelmi tisztviselő végzi. A jegyzőkönyvet az érintetti kérelemmel kapcsolatos dokumentációval együtt 5 évig kell megőrizni.

A betekintéshez való jog teljesítése nem érintheti hátrányosan mások jogait és szabadságait, ezért a személyes adatokba történő betekintés kizárólag úgy biztosítható az érintett részére, hogy más személyre vonatkozó személyes adatokat törölni, illetve anonimizálni kell, továbbá a betekintési jog biztosítására alkalmazott helyiséget úgy kell megválasztani, hogy a betekintéshez való jog gyakorlása során más személy és az érintett jogai és szabadságai ne sérüljenek.

c) Helyesbítéshez való jog

Az érintett az adatkezelés teljes ideje alatt kérheti pontatlan személyes adatainak módosítását (helyesbítését), illetve a hiányos személyes adatok kiegészítését. A helyesbítéshez való jog az adatkezelés módjától függetlenül gyakorolható, kivéve, ha e jog gyakorlása az adatkezelés jellegénél fogva nem értelmezhető (pl. kamerás megfigyelés esetén). A Társaság a helyesbítés iránti kérelem teljesítéséről köteles minden olyan címzettet tájékoztatni, akivel, vagy amellyel a személyes adatokat közölték, kivéve, ha ez lehetetlennek bizonyul vagy aránytalan nagy erőfeszítést igényel. Az érintettet kérésére a Társaság tájékoztatja e címzettekről.

A Társaság lehetőség szerint indokolatlan késedelem nélkül intézkedik a helyesbítés érdekében, és tájékoztatja az érintettet a helyesbítés tényéről és időpontjáról.

ca) A személyes adatok módosításához való jog

A személyes adatok módosításának célja a pontatlan személyes adatok helyesbítése. Pontatlannak minősül egy személyes adat, ha az nem felel meg a valóságnak, vagy más egyéb oknál fogva félrevezető. A Társaság az érintett által rendelkezésére bocsátott vagy más módon tudomására jutott információk alapján helyesbíti a pontatlan személyes adatokat.

cb) A személyes adatok kiegészítéséhez való jog

Hiányosnak minősül a személyes adat, amennyiben az összességében vagy az adatkezelés célja szempontjából nem teljes vagy megfelelő. A Társaság a rendelkezésére álló vagy az érintett által rendelkezésére bocsátott, kiegészítéshez szükséges adatok alapján a hiányos adatokat úgy módosítja, hogy azok teljessé váljanak, vagy azok mellett rögzíti a kiegészítő információkat. E részjogosítványt azonban az érintett csak abban az esetben gyakorolhatja, amennyiben az az adatkezelés céljának megfelel. Az adattakarékosság elve alapján ugyanis kizárólag a cél szempontjából szükséges, megfelelő és releváns információk kezelhetők, ezen a körön kívül eső információk felhasználása viszont a célra tekintettel túlzó.

d) Törléshez való jog („Elfeledtetéshez való jog”)

Az érintett kérheti a személyes adatainak törlését, ha

a) az adatkezelés célja megszűnt,
b) az érintett visszavonja hozzájárulását,
c) azok kezelése jogellenes,
d) az adatok tárolásának meghatározott határideje lejárt,
e) azt bíróság vagy hatóság elrendelte,
f) az érintett tiltakozott az adatkezeléssel szemben és nincs elsőbbséget élvező jogszerű ok az adatkezelésre.

Az adatkezelő az érintett kérelmének teljesítését megtagadhatja, ha a GDPR 17. cikkében foglalt valamely feltétel fennáll, így különösen az adatkezelés szükséges

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
b) a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
c) a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból;
d) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

A Társaság a törlés iránti kérelem teljesítéséről köteles minden olyan címzettet tájékoztatni, akivel, vagy amellyel a személyes adatokat közölték, kivéve, ha ez lehetetlennek bizonyul vagy aránytalan nagy erőfeszítést igényel. Az érintettet kérésére a Társaság tájékoztatja e címzettekről.

e) Az adatkezelés korlátozásához való jog

Az adatkezelés korlátozásához való jog gyakorlása az adatkezelés ideiglenes felfüggesztését jelenti. Az érintettnek kérelmében nyilatkoznia kell arról, hogy milyen indokok alapján kezdeményezi személyes adatai kezelésének korlátozását. Az érintett az alábbi négy esetben kérheti a személyes adatai kezelésének korlátozását:

a) Vitatott a személyes adat pontossága: a Társaságnak ebben az esetben indokolatlan késedelem nélkül meg kell vizsgálnia, hogy a szóban forgó személyes adatok valóban nem felelnek meg a valóságnak. Ez esetben a korlátozás arra az időtartamra vonatkozik, amíg a Társaság ellenőrzi az adatok helyességét.
b) Jogellenes adatkezelés: a személyes adatok nem a GDPR-ban foglaltaknak, illetve nem a vonatkozó egyéb előírásoknak megfelelő kezelése esetén az érintett jogosult lenne a személyes adatok törlését kérni, vagy a Társaság – a jogellenes adatkezelés megállapítása esetén – köteles lenne a személyes adatok törlésére, de az érintett ellenzi a személyes adatainak törlését.
c) Az adatkezelés célja megszűnt vagy teljesült, de az érintettnek szüksége van a személyes adatokra jogi igények előterjesztéséhez, érvényesítéséhez, védelméhez.
d) Az érintett a saját helyzetéből adódó ok miatt gyakorolja tiltakozáshoz való jogát, a Társaság csak kényszerítő erejű jogos indokok alapján kezelheti tovább a személyes adatokat.

A korlátozás addig tart, amíg azt az érintett által megjelölt indok szükségessé teszi. Ebben az esetben a személyes adatok – a tárolás kivételével – csak az érintett hozzájárulásával; vagy jogi igények előterjesztéséhez, érvényesítéséhez, védelméhez; vagy más természetes vagy jogi személy jogainak védelme érdekében; vagy fontos közérdek miatt kezelhetők. A Társaságnak az érintett kérésére történt korlátozás feloldásáról az érintettet előzetesen tájékoztatnia szükséges.

A Társaság az adatkezelés korlátozása iránti kérelem teljesítéséről köteles minden olyan címzettet tájékoztatni, akivel, vagy amellyel a személyes adatokat közölték, kivéve, ha ez lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére a Társaság tájékoztatja ezen címzettekről.

f) Az adathordozhatósághoz való jog

Az adathordozhatósághoz való jog abban az esetben gyakorolható, ha az adatkezelés keretében kezelt személyes adatokat az érintett bocsátotta az adatkezelő rendelkezésére, valamint, ha az adatkezelés automatizált módon (elektronikus úton) történik, illetve, ha az adatkezelés jogszerűsége az érintett hozzájárulásán vagy az adatkezelő és az érintett közötti szerződésen alapul. Az adatkezelő szervezeti egység köteles az automatizált módon végzett, e feltételeknek megfelelő adatkezeléseit úgy kialakítani, hogy az adathordozhatósághoz való jogot biztosítsa. Az adathordozhatósághoz való jog keretében az érintett jogosult arra, hogy tagolt, széles körben használt, géppel olvasható formátumban megkapja a rá vonatkozó személyes adatokat, illetve jogosult arra is, hogy a Társaság az általa pontosan megjelölt adatkezelő részére továbbítsa a rá vonatkozó személyes adatokat. A Társaság az

adattovábbítást követően a címzett adatkezelő által végzett adatkezelésért nem tartozik felelősséggel. Az adathordozhatósághoz való jog gyakorlása nem érintheti hátrányosan mások jogait és szabadságait.

g) A tiltakozáshoz való jog

A tiltakozáshoz való jog csak akkor gyakorolható, ha a Társaság adatkezelésének jogszerűségét a közérdekű feladat végrehajtása vagy a jogos érdek jogalapja biztosítja. A tiltakozáshoz való jog gyakorlására irányuló kérelem előterjesztése esetén a Társaság nem kezelheti tovább az érintett személyes adatait, azokat köteles törölni, kivéve, ha a Társaság bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, továbbá, ha azok jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükségesek. A Társaság a tiltakozáshoz való jog gyakorlása esetén köteles minden kérelmet egyedileg elbírálni.

h) Automatizált döntéshozatal egyedi ügyekben és profilalkotás

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

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

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

A Társaság nem végezhet olyan automatizált döntéshozatalt, amely során különleges adatok kezelése történik, kivéve, ha az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult, vagy az adatkezelés jelentős közérdek miatt szükséges, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

Amennyiben a Társaság a személyes adatokat automatizált döntéshozatal keretében kezeli, az adatkezeléssel összefüggésben tájékoztatnia kell az érintettet az automatizált döntéshozatal tényéről, ismertetnie kell az érintettel az alkalmazott logikát (a tájékoztatásnak arra kell fókuszálnia, hogy érthetően és világosan bemutassa a döntéshozatal eredményét alátámasztó megfontolásokat, tényezőket, így elsődlegesen a döntés meghozatala során figyelembe vett főbb jellemzőkre, az ilyen információk forrásának és relevanciájának ismertetésére kell szorítkozni) és tájékoztatnia kell az érintettet az adatkezelés jelentőségéről, valamint a várható következményeiről, különös tekintettel annak az érintettre gyakorolt hatásairól.

i) A hozzájárulás visszavonásához való jog

Amennyiben az adatkezelés jogszerűségét az érintett hozzájárulása biztosítja, úgy az érintett az adatkezeléshez adott hozzájárulását bármikor, korlátozás nélkül visszavonhatja. A hozzájárulás visszavonásához való jogot ugyanolyan könnyen biztosítani kell, mint ahogyan az érintett a hozzájáruló nyilatkozatát megtehette. Az adatkezelés megkezdésekor az érintettet tájékoztatni kell arról, hogy a hozzájárulása visszavonása nem érinti a hozzájárulás visszavonását megelőzően végzett adatkezelés jogszerűségét.

Ha az érintett visszavonja a hozzájárulását, a Társaság nem kezelheti többé az érintett személyes adatát. A hozzájárulás visszavonásakor a Társaságnak biztosítania kell az adatok törlését, kivéve akkor, ha másik jogalap lehetővé teszi a törléssel érintett személyes adatok kezelését. Abban az esetben, ha az érintett visszavonja a hozzájárulását, és a személyes adatokat az adatkezelő szervezeti egység másik jogalapra hivatkozással a továbbiakban is kezelni szeretné, úgy az adatkezelés csak akkor folytatható, ha az adatkezelés új jogalapja meghatározásra, és az érintett az adatkezelésről tájékoztatásra került.

j) Panasztételhez- és bírósági jogorvoslathoz való jog

Az érintett jogosult arra, hogy a Társaság által végzett adatkezeléssel kapcsolatosan panaszt terjesszen elő a NAIH-nál, illetve bírósághoz forduljon.

Amennyiben az érintett a jelen pontban foglalt jogának gyakorlását megelőzően – érintetti kérelemnek nem minősülő – panasszal fordul a Társasághoz, úgy a panasz elbírálására és megválaszolására a jelen fejezetben foglaltakat megfelelően kell alkalmazni.

4.5.2. Az érintetti jogok gyakorlására vonatkozó szabályok

Érintetti jog gyakorlására irányuló kérelmet (a továbbiakban a jelen fejezet keretében: kérelem) terjeszthet elő:

a) az érintett személyesen vagy meghatalmazott útján,
b) a kiskorú érintett önállóan a tájékoztatáshoz-, a hozzáféréshez-, a helyesbítéshez-, a korlátozáshoz-, a tiltakozáshoz- és az adathordozhatósághoz való jogát illetően, valamint a törléshez való jogát illetően a törvényes képviselőjével közösen,
c) a kiskorú érintett törvényes képviselője bármely érintetti jogot illetően,
d) az érintett halálát követő öt éven belül a 4.5.2.3. pontban megjelölt személyek.

Amennyiben az érintett a kérelmét képviselő útján terjesztette elő, úgy a kérelem kizárólag akkor teljesíthető a képviselő részére, ha a képviseleti jogosultság teljes kétséget kizáróan megállapításra került. Amennyiben a képviseleti jogot írásbeli meghatalmazás keletkezteti, úgy a képviseleti jogot igazoltnak kell tekinteni, ha az elektronikus úton megküldött kérelemhez a meghatalmazás elektronikus másolatát mellékletként csatolják. A képviseleti jogosultság kétséget kizáró megállapítása érdekében a kérelmet beküldő személyt (feltételezett képviselőt) írásban fel kell hívni a képviseleti jogának igazolására. Amennyiben a feltételezett képviselő a képviseleti jogát nem tudja kétséget kizáróan igazolni, úgy az előterjesztett kérelemben megjelölt érintettet – amennyiben az érintett a kérelem alapján azonosítható és az érintettel történő kapcsolatfelvételhez szükséges adatok rendelkezésre állnak – tájékoztatni kell arról, hogy a képviseletében kérelmet terjesztettek elő, de a képviselő azonosítása sikertelen volt. Amennyiben az érintett a képviseleti jogot igazolja, úgy az érintetti kérelem – amennyiben a teljesítésnek egyéb akadálya nem áll fenn – teljesíthető a képviselő részére.

4.5.2.1. Az érintetti jogok gyakorlásának módja

Az érintett a kérelmét szóban (telefonon vagy személyesen) vagy írásban (postai úton vagy elektronikus úton) terjesztheti elő. A kérelem akkor minősül beérkezettnek, amikor a szóban (telefonon vagy személyesen) benyújtott igény a 9. számú függelék szerint rögzítésre, az írásban, postai úton benyújtott igény az iratkezelési szabályok szerint érkeztetésre kerül, illetve amikor az elektronikus úton benyújtott igény a Társaság elektronikus postafiókjába beérkezik. Amennyiben az igény szóban érkezik, úgy a Társaság azon munkavállalója, akivel az igényt közölték, köteles az igényről haladéktalanul, a 9. számú függelék szerint feljegyzést készíteni, és haladéktalanul megküldeni az adatkezelő szervezet és az adatvédelmi tisztviselő részére, az adatvedelem@mav-start.hu e-mail címre. Amennyiben a feljegyzést készítő munkavállaló nem tudja meghatározni azt,

hogy a Társaság mely szervezeti egysége minősül adatkezelő szervezeti egységnek, úgy a feljegyzést az adatvédelmi tisztviselő részére küldi meg. Amennyiben az érintett a kérelmet nem az adatvédelmi tisztviselő részére küldte, úgy a kérelem címzettje köteles azt haladéktalanul, de legkésőbb 3 munkanapon belül továbbítani az adatvedelem@mav-start.hu e-mail címre.

Amennyiben az érintett a kérelmét az Ügyfélszolgálat szervezet részére – szóban, ideértve a telefonos utat is, vagy írásban, ideértve az elektronikus utat is – terjesztette elő, úgy a kérelmet kezelő ügyfélszolgálati munkavállaló – az alábbi kivétellel – haladéktalanul, de legkésőbb három munkanapon belül továbbítja a kérelmet, illetve a szóban előterjesztett kérelemről felvett jegyzőkönyvet az adatvédelmi tisztviselő részére az adatvedelem@mav-start.hu e-mail címre.

Az adatvédelmi tisztviselő részére nem szükséges továbbítani az alábbi érintetti jog gyakorlására irányuló kérelemnek is minősülő:

a) a Társaság által üzemeltetett kamerák által rögzített kamerafelvételekkel kapcsolatos,
b) a MÁV Zrt. vagy a Társaságtól eltérő jogi személy által üzemeltetett kamerák által rögzített kamerafelvételekkel kapcsolatos,
c) az egyértelműen nem a MÁV Személyszállítási Zrt. tevékenységét érintő,
d) a személyes adatok helyesbítésére irányuló, saját hatáskörben elbírálható és teljesíthető

kérelmeket.

Az a) és b) pont szerint előterjesztett kérelmekről a kérelmek kezelésére külön utasítás szerint kijelölt szervezet havonta elektronikus úton az adatvedelem@mav-start.hu email címre adatszolgáltatást teljesít az adatvédelmi tisztviselő részére, amelyben tájékoztatást ad az érintettek által előterjesztett kérelmek számáról, teljesítéséről vagy a teljesítés elmaradásáról, utóbbi esetben a teljesítés elmaradásának okáról.

Amennyiben az a) – d) pontban foglaltak szerint előterjesztett kérelem az adatvédelmi tisztviselő részére továbbításra kerül, úgy az adatvédelmi tisztviselő a jelen pontban foglaltak szerint közreműködik a kérelem megfelelő teljesítésében.

4.5.2.2. Az érintetti jog gyakorlására irányuló kérelem teljesítése

Amennyiben az érintett a kérelmet az adatvédelmi tisztviselő részére terjesztette elő, úgy az adatvédelmi tisztviselő a kérelem beérkezését követően elektronikus úton – emailben – haladéktalanul, de legkésőbb három munkanapon belül – az érintetti kérelem teljesíthetőségének vizsgálatára és annak teljesítésére vonatkozó szükséges tájékoztatások megadásával – továbbítja a kérelemben megjelölt adatkezelési folyamatban érintett adatkezelő szervezeti egység részére.

Az adatkezelő szervezeti egység a kérelem beérkezését követően haladéktalanul, de legfeljebb 5 munkanapon belül megvizsgálja a kérelem teljesíthetőségét. Az adatkezelő szervezeti egység a kérelem teljesíthetőségének vizsgálata, valamint az érintett részére küldött válasz előkészítése során folyamatosan együttműködik az adatvédelmi tisztviselővel.

A kérelem teljesíthetősége keretében az adatkezelő szervezeti egység elsősorban meggyőződik arról, hogy a kérelmező olyan személynek minősül-e, akinek a személyes adatát kezeli. Ennek megállapításához a kérelmezőt – a Társaság által kezelt személyes adatok alapján – azonosítania kell. Amennyiben az adatkezelő szervezeti egység nem tudja azonosítani a kérelmezőt, úgy a kérelmező azonosításához szükséges kiegészítő információk szolgáltatását kérheti. Kiegészítő információként kizárólag olyan információ kérhető, amelyet a Társaság személyes adatként kezel. Amennyiben a kiegészítő információk alapján sem azonosítható az érintett, úgy meg kell győződni arról, hogy a Társaság más adatkezelő szervezeti egysége nem kezeli-e az érintett személyes adatát. Amennyiben a kérelmező nem azonosítható, úgy a kérelmét el kell utasítani.

Az adatkezelő szervezeti egység az érintett azonosítását követően tartalmi szempontból megvizsgálja az érintett által előterjesztett kérelmet és megállapítja, hogy az érintett mely érintetti jogát/jogait gyakorolja. Ezt követően meg kell állapítani azt, hogy az érintett által előterjesztett kérelem melyik, a Társaság által végzett adatkezelést/adatkezeléseket érinti. A kérelemben érintett adatkezelési folyamatok azonosítását követően – az adatkezelés jogalapjára tekintettel – meg kell vizsgálni, hogy az érintett jogosult-e gyakorolni a kérelmében megjelölt érintetti jogot/jogokat.

Amennyiben megállapításra kerül, hogy az érintett jogosult gyakorolni az érintetti jogait, úgy az adatkezelő szervezeti egység megvizsgálja, hogy a kérelemben gyakorolt érintetti jog alapján a kérelem részben vagy egészben teljesíthető, vagy a kérelmet el kell utasítani. Amennyiben a kérelem teljesíthető, úgy meg kell vizsgálni, hogy a kérelem teljesítéséhez milyen intézkedés megtételére van szükség. A kérelem részben vagy egészben történő teljesíthetőségének, illetve elutasításának megállapítása során a 4.5.1. pontban foglaltak irányadóak.

Amennyiben az érintetti jog gyakorlására irányuló kérelem vagy az érintett által előterjesztett panasz vizsgálata során felmerül a Társaság munkavállalójának munkaviszonyból származó vétkes kötelezettségszegése vagy ennek alapos gyanúja és az érintetti jog gyakorlására irányuló kérelem vagy az érintett által előterjesztett panasz vizsgálatához a Társaság valamely munkavállalójának személyes meghallgatása szükséges, úgy a meghallgatást az adatvédelmi tisztviselő a Humánerőforrás Főigazgatóság Munkajog szervezetének közreműködésével tartja meg, amelyről jegyzőkönyvet kell készíteni. A meghallgatás megszervezésére és lebonyolítására a Kollektív Szerződésben külön utasításban foglalt szabályok megfelelően alkalmazandók.

Az adatkezelő szervezeti egység az érintett kérelmét indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül megválaszolja. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő szervezeti egység a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül írásban tájékoztatja az érintettet.

Amennyiben az érintett elektronikus úton nyújtotta be a kérelmét, úgy a kérelmet elektronikus úton kell megválaszolni, kivéve, ha az érintett azt másként kéri. Amennyiben a kérelem az adatvédelmi tisztviselőhöz érkezett be, úgy a kérelemre adott válasz az adatvédelmi tisztviselő közreműködésével küldhető ki. Az elektronikus úton, e-mailben érkezett kérelmeket az adatvedelem@mav-start.hu e-mail címről kell megválaszolni. A szóban – ideértve a telefonos utat is – előterjesztett érintetti jog gyakorlására irányuló kérelem kizárólag akkor teljesíthető, ha az adatkezelő szervezeti egység a kérelem teljesíthetőségével kapcsolatos, a jelen utasításban foglalt feladatokat maradéktalanul el tudja végezni.

Az adatkezelő szervezeti egység a kérelem tekintetében hozott intézkedésekről tömör, átlátható, érthető, világosan és közérthetően megfogalmazott módon ad tájékoztatást az érintett részére adott válaszában. A válaszlevélben tájékoztatni kell az érintettet az őt megillető jogorvoslati jogokról, így arról, hogy panasszal élhet az adatvédelmi felügyeleti hatóságnál, illetve élhet a bírósági jogorvoslathoz való jogával. A tájékoztatásnak ki kell terjednie a jogorvoslati szervek valamennyi elérhetőségére is, ideértve a NAIH elérhetőségeit, valamint a bírósági illetékesség esetében az alábbi linkre történő utalást: https://birosag.hu/birosag-kereso.

A Társaság az érintett kérelmének teljesítését díjmentesen biztosítja. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, a Társaság, - figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre, - észszerű összegű díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő intézkedést. A költségtérítés mértékét az adatkezelő szervezeti egységnek a Társaság Gazdasági Főigazgatóságával egyeztetve kell megállapítani és a kérelmező felé igazolnia kell.

Az érintetti jogok gyakorlásával, elbírálásával és teljesítésével összefüggésben végzett adatkezelésre vonatkozó adatkezelési tájékoztatót a Társaság honlapján közzé kell tenni. Az adatkezelési tájékoztató elkészítéséért az adatvédelmi tisztviselő felelős.

A Társaság az érintetti jogok gyakorlásának elősegítése érdekében formanyomtatványokat alkalmazhat. Formanyomtatvány alkalmazása esetén azokat a Társaság honlapján közzé kell tenni. A kérelem elbírálása nem utasítható vissza kizárólag amiatt, hogy azt az érintett nem a közzétett formanyomtatványon terjesztette elő.

4.5.2.3. A személyes adatokkal összefüggő jogok érvényesítése az érintett halálát követően

Az érintett halálát követően az érintettet életében megillető érintetti jogokat elsősorban az érintett által ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal meghatalmazott személy (a továbbiakban: elhunyt által meghatalmazott személy) gyakorolhatja. Amennyiben az érintett több nyilatkozatot tett a Társaságnál, úgy a későbbi időpontban tett nyilatkozatban meghatalmazott személy jogosult eljárni. Az elhunyt által meghatalmazott személy az Infotv. hatálya alá tartozó adatkezelések esetén a hozzáféréshez-, helyesbítéshez-, korlátozáshoz- és törléshez való jogot, míg a GDPR hatálya alá tartozó adatkezelések esetén a hozzáféréshez-, helyesbítéshez-, korlátozáshoz-, törléshez- és tiltakozáshoz való jogot gyakorolhatja. Az elhunyt által meghatalmazott személy hiányában az elhunytat életében megillető egyes jogokat az érintett azon közeli hozzátartozója jogosult gyakorolni, aki azok gyakorlására első alkalommal terjeszt elő kérelmet a Társaság részére. A közeli hozzátartozó az Infotv. hatálya alá tartozó adatkezelések esetén a helyesbítéshez való jogot, míg a GDPR hatálya alá tartozó adatkezelések esetén a helyesbítéshez- és tiltakozáshoz való jogot, valamint ha az adatkezelés már az érintett életében is jogellenes volt vagy az adatkezelés célja az érintett halálával megszűnt a törléshez- és a korlátozáshoz való jogot gyakorolhatja.

Amennyiben az elhunyt személyes adataira vonatkozóan nyújtanak be kérelmet, úgy az adatkezelő szervezeti egység haladéktalanul megvizsgálja a kérelem teljesíthetőségét, és a kérelem beérkezéséről tájékoztatja az adatvédelmi tisztviselőt.

A kérelem teljesíthetőségének keretében az adatkezelő szervezeti egység elsősorban meggyőződik arról, hogy a kérelem valóban olyan érintettre vonatkozik-e, akinek a személyes adatát a Társaság kezeli. Ehhez a Társaság valamennyi szervezeti egysége által vezetett nyilvántartás ellenőrzésére szükség van.

Amennyiben a kérelemben megjelölt elhunyt személy személyes adatát a Társaság kezeli, úgy az adatkezelő szervezeti egység haladéktalanul ellenőrzi, hogy a kérelmező az elhunyt közeli hozzátartozójának vagy az elhunyt által meghatalmazott személynek minősül-e. Az adatkezelő szervezeti egység az érintett elhalálozása tényének és idejének ellenőrzése céljából kérheti a kérelmezőtől az érintett elhalálozását igazoló dokumentum (halotti anyakönyvi kivonat vagy bírósági határozat) bemutatását. A kérelmező saját személyazonosságát közokirattal (személyazonosításra alkalmas okmány), illetve a közeli hozzátartozói viszonyt (közeli hozzátartozónak minősül a házastárs, az egyeneságbeli rokon, az örökbefogadott, a mostoha- és a nevelt gyermek, az örökbefogadó-, a mostoha- és a nevelőszülő és a testvér) szintén közokirattal (a közeli hozzátartozói minőségtől függően házassági anyakönyvi kivonat vagy születési anyakönyvi kivonat) igazolja.

Az azonosítás történhet személyes megjelenés mellett vagy az azonosításhoz szükséges okiratok adatkezelő szervezeti egység részére elektronikus úton történő megküldésével és megtekintésével. Az azonosítást 24 órán belül el kell végezni. Az azonosításról feljegyzést kell készíteni. Az azonosításhoz szükséges dokumentumokat és a dokumentumot tartalmazó elektronikus levelet az azonosítást és a feljegyzés elkészítését követően haladéktalanul törölni kell.

A kérelem teljesítésére a 4.5.2.2. pontban foglaltakat megfelelően alkalmazni kell azzal, hogy a kérelmet annak benyújtásától számított legrövidebb időn, de legfeljebb 25 napon belül kell megválaszolni. A válaszadásra nyitva álló határidő meghosszabbítására nincs lehetőség.

4.6. Az adatkezeléssel kapcsolatos feladatok és kötelezettségek

Az adatkezelő szervezeti egység az adatkezelés megkezdését megelőzően – az adatkezelés megkezdésétől az adatkezelés befejezéséig – köteles megtervezni az adatkezelési folyamatot, amelynek keretében az alábbi részfeladatokat végzi el:

a) Elemzi az adatkezelési folyamat kockázatait, szükség esetén hatásvizsgálatot végez.
b) Meghatározza az adatkezelés jogszerűségét biztosító jogalapot és a választott jogalap függvényében elvégzi a szükséges dokumentációs kötelezettségeket.
c) Az adatkezelési folyamat megkezdését megelőzően a kockázatelemzés során azonosított kockázatok kezelése érdekében meghatározott adatbiztonsági intézkedéseket végrehajtja.
d) Elkészíti az adatkezelési folyamat tekintetében irányadó adatkezelési tájékoztatót és meghatározza az adatkezelési tájékoztató érintettel történő közlésének módját.
e) Az adatkezelés megkezdését követően az adatkezelési folyamatban bekövetkező változás esetén az adatkezelési folyamatot – a jelen utasításban foglaltaknak megfelelően – felülvizsgálja.
f) Az adatkezelési folyamat befejezését követően gondoskodik a személyes adatok törléséről, illetve a személyes adatokat tartalmazó adathordozók megsemmisítéséről.

Az a) – f) pontban foglalt részfeladatokra vonatkozó részletszabályokat a jelen fejezet egyes alfejezetei határozzák meg.

4.6.1. Az adatkezelési folyamat tervezése, az adatkezeléssel járó kockázatok elemzése

4.6.1.1. A kockázatelemzés elvégzésének módja, a kockázatok elemzésének szempontjai

A személyes adatok kezelésével járó tevékenység tervezési folyamata során az adatkezelő szervezeti egységnek elemeznie kell azt, hogy az adatkezelés a természetes személyek jogaira és szabadságaira nézve milyen valószínűségű és súlyosságú kockázattal jár. Amennyiben az adatkezelési folyamat több adatkezelő szervezeti egységet érint, a kockázatelemzésbe valamennyi adatkezelő szervezeti egységet be kell vonni. A kockázatelemzésbe az adatkezelő szervezeti egység által az Adatvédelmi munkacsoportba delegált tagot és az adatvédelmi tisztviselőt minden esetben be kell vonni. Amennyiben az adatkezelési folyamat keretében informatikai eszközök alkalmazására is sor kerül, az adatvédelmi kockázatelemzésbe a Biztonsági Főigazgatóság információvédelmi szakterületét be kell vonni.

A kockázat valószínűségét és súlyosságát (hatását) az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében – objektív, a Társaság érdekeit mellőző értékelés keretében – kell meghatározni. A kockázatelemzés megfelelő elvégzéséhez az adatkezelési folyamat tervezésekor meg kell határozni az adatkezelési folyamat és azon belül – amennyiben az elkülöníthető – az egyes részfolyamatok pontos célját, az adatkezeléssel érintett személyes adatok körét, az adatkezelés módját (elektronikus és/vagy papír alapon), ideértve az adatkezelés technikai megvalósítását (rendszer, szoftver stb. vagy ezek használata nélkül), valamint az adatkezelés tervezett időtartamát és az adatkezelés jogalapját. Kizárólag olyan személyes adatok kezelésére kerülhet sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek, ez vonatkozik a személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. A kockázatelemzés keretében ki kell térni arra is, hogy az adatkezeléshez szükséges-e adatfeldolgozó igénybe vétele, amennyiben igen, úgy be kell mutatni az adatfeldolgozó által végzett adatfeldolgozást. A kockázatelemzésben meg kell határozni a személyes adatokhoz való hozzáférési jogosultságokat is. A kockázatelemzésben ki kell térni a természetes személy jogaira és szabadságaira jelentett,

változó valószínűségű és súlyosságú kockázatok figyelembe vételére is. Az adatkezelés kockázat(ai)ának felmérését az 5. számú függelékben található dokumentum kitöltésével szükséges elvégezni Az adatvédelmi tisztviselő szükség esetén állásfoglalást bocsáthat ki a további értékelési szempontok meghatározására.

A kockázatelemzés keretében megállapított kockázatok alapján az adatkezelő szervezeti egység az adatkezelés folyamatának tervezése során meghatározza a kockázatok kezeléséhez szükséges technikai és szervezési intézkedéseket. Az automatizált módon végzett adatkezelés esetén az IBSZ-ben foglalt adatbiztonsági rendelkezéseket alkalmazni kell. A biztonság megfelelő szintjének meghatározásakor figyelembe kell venni az olyan kockázatokat, amelyek a személyes adatok megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

Az adatkezelő szervezeti egység minden új, korábban nem létező cél szerinti adatkezelés bevezetése előtt köteles kockázatelemzést, amennyiben szükséges úgy hatásvizsgálatot is végezni. Meglévő adatkezelés esetén az adatkezelő szervezeti egység az adatvédelmi kockázatelemzést háromévente köteles felülvizsgálni. Az adatvédelmi kockázatelemzés harmadik felülvizsgálatát követően új adatvédelmi kockázatelemzést kell elvégezni. A kockázatelemzés felülvizsgálatát, illetve az új kockázatelemzést – a kockázatelemzés elvégzésének indokát képező tény bekövetkezését követő – 30 napon belül el kell végezni. Amennyiben az adatvédelmi folyamat bármely része megváltozik, az adatkezelés kockázatelemzését felül kell vizsgálni, kivéve, ha az adatkezelés célja, a kezelt adatok köre, az adatkezelés módja vagy az adatkezelés időtartama változik meg, ez esetben új kockázatelemzést kell elvégezni. A kockázatelemzés felülvizsgálatát, illetve az új kockázatelemzést az adatkezelési folyamat módosításának tervezése során kell elvégezni.

Amennyiben a kockázatok elemzése vagy a kockázatelemzés felülvizsgálata során megállapításra kerül, hogy az adatkezelés a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal jár, úgy adatvédelmi hatásvizsgálatot szükséges elvégezni. Amennyiben az adatkezelő szervezeti egység a kockázatok értékelése alapján megállapítja, hogy az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, de úgy dönt, hogy az adatvédelmi hatásvizsgálat elvégzését mellőzi, úgy dokumentáltan alá kell támasztania az adatvédelmi hatásvizsgálat mellőzésének okait, és arról ki kell kérnie az adatvédelmi tisztviselő véleményét.

A kockázatelemzést és annak felülvizsgálatát az 5. számú függelék szerinti nyomtatványon szükséges elvégezni. A formanyomtatvány szövegétől az adatkezelési folyamat jellege és körülményei alapján el lehet térni. Az elvégzett kockázatelemzést az adatkezelési folyamattal érintett adatkezelési szervezeti egység vezetője hagyja jóvá. A kockázatelemzésről készült dokumentumokat az adatkezelési folyamat befejezését követő 10 évig meg kell őrizni. Az elvégzett kockázatelemzést az adatvédelmi tisztviselőnek – elektronikus úton – meg kell küldeni.

4.6.1.2. A kockázatelemzésre vonatkozó átmeneti rendelkezések

A jelen utasítás hatálybalépésekor folyamatban lévő adatkezelési folyamatok kockázatelemzését a hatályba lépést követő második év végéig el kell végezni. Az e határidőig elvégzett kockázatelemzések arányát az adatvédelmi tisztviselő az éves beszámolójában ismerteti. Az elvégzett kockázatelemzések tekintetében a 4.6.1.1. pontban foglalt rendelkezéseket alkalmazni kell.

A jelen Utasítás hatálybalépésekor folyamatban lévő adatvédelmi megfelelőségi vizsgálatra a vizsgálat megkezdésekor hatályos Utasításban foglalt rendelkezéseket kell alkalmazni. A jelen Utasítás hatályba lépését megelőzően elvégzett vagy folyamatban lévő adatvédelmi megfelelőségi vizsgálat(ok) monitoring vizsgálatára a jelen Utasításban foglaltakat kell alkalmazni.

4.6.2. Adatvédelmi hatásvizsgálat

Amennyiben az adatkezelő szervezeti egység a személyes adatok kezelésével járó tevékenység tervezésekor úgy ítéli meg, hogy az érintettek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal jár, akkor a tervezési folyamat részeként adatvédelmi hatásvizsgálatot kell végeznie. Egymáshoz hasonló adatkezelési műveletek, amelyek hasonló kockázatokat jelentenek egyetlen egy hatásvizsgálat keretében is elvégezhetők. Az adatvédelmi hatásvizsgálat lefolytatásába, valamint az elvégzett hatásvizsgálat felülvizsgálatába az adatvédelmi tisztviselőt be kell vonni.

Az adatkezelő szervezeti egység az adatvédelmi hatásvizsgálatot rendszeres időközönként, de legalább háromévente, dokumentált módon felülvizsgálja. A felülvizsgálatot el kell végezni, ha az adatkezelési folyamat valamely lényeges körülménye, így az adatkezelés jellege, hatóköre, célja, időtartama, a kezelt személyes adatok köre, az adatkezelésben részt vevő adatkezelők köre – ideértve a címzetteknek történő adattovábbítást is, kivéve, ha a címzettnek történő adattovábbítás megszüntetésére kerül sor –, az adatkezelési folyamat során alkalmazott adatbiztonsági intézkedések és az adatkezelés során alkalmazott technológia megváltozik.

Az adatkezelő szervezeti egység az adatvédelmi hatásvizsgálat során kikéri az érintettek (pl. munkavállalók) vagy képviselőik (pl. szakszervezet) véleményét a tervezett adatkezelésről. Mellőzhető az érintettek véleményének kikérése, ha az által a Társaság üzleti tervének titkossága sérülne, illetve aránytalan terhet jelentene, vagy kivitelezhetetlen lenne ez az intézkedés. Amennyiben az adatkezelő szervezeti egység úgy dönt, hogy nem kéri ki az érintettek véleményét, akkor e döntését dokumentált módon alá kell támasztania.

4.6.2.1. Az adatvédelmi hatásvizsgálat elvégzésének kötelező esetei

Az adatkezelő szervezeti egység adatvédelmi hatásvizsgálatot végez el, ha az adatkezelés során
- a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelésére kerül sor, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek,
- a személyes adatok különleges kategóriái vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelésére kerül sor,
- a nyilvános helyek nagymértékű, módszeres megfigyelésére kerül sor, vagy
- a tervezett adatkezelési művelet szerepel az adatvédelmi felügyeleti hatóság által közzétett, kötelező eseteket tartalmazó listán.

4.6.2.2. Az adatvédelmi hatásvizsgálat mellőzésének esetei

Az adatkezelő szervezeti egység mellőzi az adatvédelmi hatásvizsgálat elvégzését, ha
- az adatkezelés valószínűsíthetően nem jár magas kockázattal a természetes személyek jogaira és szabadságaira nézve,
- az adatkezelés jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít egy olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat, ilyen esetekben felhasználhatók a Társaság által korábban elvégzett, hasonló adatkezelés adatvédelmi hatásvizsgálatának eredményei,
- az adatkezelési műveleteket a Hatóság 2018. május előtt már ellenőrizte, és az adatkezelés feltételei azóta nem változtak meg,
- az adatkezelés jogszerűségét a GDPR 6. cikk (1) bekezdés c) vagy e) pontjában foglalt jogalap biztosítja és a vonatkozó jogszabály szabályozza az adott adatkezelési műveletet, valamint e

jogszabály alapján végzett adatkezelésre már készült adatvédelmi hatásvizsgálat, feltéve, hogy a jogszabály kifejezetten nem rögzíti a hatásvizsgálat elvégzésének kötelezettségét,
- az adatkezelés szerepel a Hatóság által összeállított, a nem kötelező adatkezelési műveletek jegyzékében, amelyekre tekintettel nem kötelező hatásvizsgálatot készíteni.

4.6.2.3. Az adatvédelmi hatásvizsgálat lefolytatása és az előzetes konzultáció

Az adatkezelő szervezeti egység az adatvédelmi hatásvizsgálatot a jelen utasítás 6. számú függeléke alapján vagy az adatvédelmi felügyeleti hatóság által elérhetővé tett adatvédelmi hatásvizsgálati szoftver igénybevételével folytatja le.

Az adatvédelmi hatásvizsgálat célja, hogy az adatkezelő szervezeti egység azonosítsa az adatkezelési folyamatban felmerülő valamennyi kockázatot és megfelelő intézkedések meghozatalával csökkentse, kiküszöbölje azokat. Amennyiben megállapításra kerül, hogy a kockázat mérséklése céljából meghatározott intézkedések hiányában az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira, és az adatkezelő szervezeti egység véleménye alapján a kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon, úgy az adatkezelő szervezeti egység – az adatvédelmi tisztviselő útján – előzetes konzultációt kezdeményez az adatvédelmi felügyeleti hatósággal.

Az előzetes konzultáció során az adatkezelő szervezeti egység tájékoztatást ad az adatvédelmi felügyeleti hatóság részére különösen az alábbiakról:
- az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről,
- a tervezett adatkezelés céljairól és módjairól;
- az érintettek a GDPR értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;
- az adatvédelmi tisztviselő elérhetőségeiről;
- az adatvédelmi hatásvizsgálatról;
- a felügyeleti hatóság által kért minden egyéb információról.

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

4.6.3. Az adatkezelés adatvédelmi jogi megfelelőségének biztosításával kapcsolatos kötelezettségek

4.6.3.1. Az adatkezelő személyének meghatározása

Az adatkezelő szervezeti egység az adatkezelési folyamat tervezése során – amennyiben az adatkezelési folyamatban az adatkezelőn kívül harmadik személy (a továbbiakban: harmadik személy) is részt vesz – köteles minősíteni az adatkezelési folyamatban részt vevő személyeket. A minősítést a 4. számú függelékben foglalt szempontrendszer figyelembevételével kell elvégezni. A minősítés elvégzése során az adatvédelmi tisztviselő állásfoglalása kikérhető.

Amennyiben a minősítés alapján megállapításra kerül, hogy a harmadik személy a Társaság adatfeldolgozójának minősül, úgy az adatkezelő szervezeti egység gondoskodik az adatfeldolgozási megállapodás előkészítéséről és megkötéséről. Az adatfeldolgozási megállapodás – az alapjogviszonyt keletkeztető megállapodástól függetlenül – önállóan is megköthető. Az adatfeldolgozási megállapodásban foglaltaknak meg kell felelnie a GDPR 28. cikk (3) bekezdésében

foglalt követelményeknek, illetve az egyes rendelkezéseket olyan formában kell megfogalmazni, hogy a Társaság, mint adatkezelő teljesíteni tudja az adatkezelés tekintetében felelősségi körébe tartozó kötelezettségeit. Az adatvédelmi tisztviselő gondoskodik arról, hogy a Társaság rendelkezésére álljon a GDPR-nak megfelelő tartalmú adatfeldolgozási megállapodás minta. Az adatfeldolgozási megállapodásokat – függetlenül attól, hogy az ügyleti szerződés tartalmazza, vagy külön megállapodás –, azok megkötése előtt az adatvédelmi tisztviselővel előzetesen véleményeztetni kell.

Amennyiben a minősítés alapján megállapításra kerül, hogy a harmadik személy(ek) és a Társaság közös adatkezelőnek minősül (a továbbiakban együtt: a közös adatkezelésben részes társaságok), úgy a közös adatkezelésben részes társaságok közösen kötelesek előkészíteni a közös adatkezelésről szóló megállapodást.

Az adatfeldolgozási megállapodás és a közös adatkezelésről szóló megállapodás elkészítésének kötelezettsége az adatkezelő szervezeti egységet terheli, de a megállapodásokkal kapcsolatos egyeztetésekre az adatvédelmi tisztviselőt kötelező meghívni. Az adatvédelmi tisztviselő szükség esetén – az adatkezelő szervezeti egység tájékoztatása mellett – önállóan is jogosult képviselni a Társaság álláspontját a megállapodások előkészítésével összefüggő egyeztetések során.

4.6.3.2. Az adatkezelés jogalapjának meghatározása

Az adatkezelő szervezeti egység az adatkezelési folyamat tervezése során, legkésőbb az adatkezelés megkezdéséig meghatározza az adatkezelés jogalapját. Az adatkezelés jogalapjának meghatározása során ki kell kérni az adatvédelmi tisztviselő szakmai álláspontját.

Az adatkezelés jogalapjának meghatározása során az alábbi szempontokat – az alább megjelölt sorrendben és a jelen utasítás 4.4. pontjában foglaltak alkalmazása mellett – szükséges figyelembe venni.

a) Vizsgálni kell azt, hogy az adatkezelés az érintett létfontosságú érdekeinek védelme miatt szükséges-e. Amennyiben igen, úgy az adatkezelés jogszerűségét a GDPR 6. cikk (1) bekezdés d) pontja szerinti jogalap biztosíthatja.
b) Vizsgálni kell azt, hogy az adatkezelés jogi kötelezettség teljesítése érdekében szükséges-e. Amennyiben igen, úgy az adatkezelés jogszerűségét a GDPR 6. cikk (1) bekezdés c) pontja szerinti jogalap biztosíthatja.
c) Vizsgálni kell azt, hogy az adatkezelés valamely közérdekű feladat végrehajtásához szükséges-e. Amennyiben igen, úgy az adatkezelés jogszerűségét a GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap biztosíthatja.
d) Vizsgálni kell azt, hogy az adatkezelés az adatkezelő és az érintett között létrejött szerződés teljesítéséhez vagy a szerződés létrejöttéhez szükséges lépések megtétele keretében szükséges-e. Amennyiben igen, úgy az adatkezelés jogszerűségét a GDPR 6. cikk (1) bekezdés b) pontja szerinti jogalap biztosíthatja.
e) Vizsgálni kell azt, hogy az adatkezelés jogszerűségét az érintett hozzájárulása biztosíthatja-e. Amennyiben igen, úgy az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés a) pontja szerinti hozzájárulás.
f) Ha az adatkezelés jogalapjaként az adatkezelő vagy harmadik személy jogos érdeke került meghatározásra [GDPR 6. cikk (1) bekezdés f) pont], úgy az adatkezelő szervezeti egység a 7. számú függelékben foglaltak szerint érdekmérlegelési tesztet végez el az adatkezelés jogszerűségének alátámasztásához. Az érdekmérlegelési teszt elvégzése során azt kell vizsgálni, hogy melyek azok a körülmények, amelyek az adatkezelést az érintett jogainak és szabadságainak védelmével szemben indokolják. Az érdekmérlegelési teszt elvégzése során ki kell kérni az adatvédelmi tisztviselő szakmai álláspontját. Az elvégzett érdekmérlegelési tesztet az adatkezelő szervezeti egység és az adatvédelmi tisztviselő az adatkezelési folyamat végéig dokumentált módon megőrzi. Az érdekmérlegelési tesztet – kifejezetten erre irányuló igény esetén az érintett rendelkezésére kell bocsátani.

Az adatkezelés jogalapjának meghatározását követően meg kell vizsgálni, hogy az adatkezelési folyamat keretében történik-e a személyes adatok különleges kategóriájába tartozó személyes adat kezelése. Amennyiben igen, úgy elsődlegesen vizsgálni kell azt, hogy a személyes adatok különleges kategóriájába tartozó személyes adat kezelése nélkül az adatkezelés célja elérhető-e. Ha igen, akkor a személyes adatok különleges kategóriájába tartozó személyes adat kezelését mellőzni kell. Ha az adatkezelés célja nem érhető el a személyes adatok különleges kategóriájába tartozó személyes adat kezelése nélkül, akkor az ilyen személyes adat kezelése jogszerűségének biztosításához a GDPR 9. cikk (2) bekezdésében meghatározott valamely feltétel fennállását igazolni kell, ennek hiányában a személyes adatok különleges kategóriájába tartozó személyes adat kezelése tilos.

4.6.3.3. Az előzetes tájékoztatási kötelezettség teljesítése és az adatkezelési tájékoztató

A Társaságot terhelő előzetes tájékoztatási kötelezettséggel kapcsolatos feladatokat az adatkezelő szervezeti egység látja el. Ennek keretében az adatkezelő szervezeti egység az adatkezelési folyamat tervezését követően az 1. számú függelékben foglalt minta alapján – az adatvédelmi tisztviselő közreműködésével – elkészíti az adatkezelési tájékoztatót. Az 1. számú függelék szerinti adatkezelési tájékoztató minta szövegétől az adatkezelési folyamat jellegére és az adatkezelés körülményeire tekintettel el lehet térni. Amennyiben ugyanazon adatkezelési folyamat keretében a GDPR 13. és 14. cikkei szerinti tájékoztatást is meg kell valósítani, úgy egy adatkezelési tájékoztató elkészítése szükséges az 1. számú függelék tartalma szerint.

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

I. Az adatkezelési tájékoztató közlésére vonatkozó szabályok:

Az adatkezelési tájékoztató közlésének kötelezettségére vonatkozó szabályokat – a jelen utasításban foglaltak figyelembevétele mellett – az adatkezelési folyamat tekintetében irányadó utasításban úgy kell meghatározni, hogy a Társaság igazolni tudja az adatkezelésre vonatkozó információk rendelkezésre bocsátására vonatkozó kötelezettségének teljesítését. A tájékoztatási kötelezettség teljesítéséhez az adatkezelésre irányadó adatkezelési tájékoztató érintett részére történő megismerhetővé tételére van szükség. Amennyiben az adatkezelés jogszerűségét az érintett hozzájárulása biztosítja, az adatkezelési tájékoztatót a hozzájáruló nyilatkozat megtételét megelőzően, de legkésőbb azzal egyidőben meg kell ismertetni. A hozzájáruláson alapuló adatkezelés esetén az érintettet az adatkezelési tájékoztató megismeréséről minden esetben igazolható módon nyilatkoztatni kell.

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

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

Amennyiben az adatkezelés keretében az adatkezelő szervezeti egység a személyes adatokat papír alapú dokumentum keretében gyűjti és az adatkezelés körülményeire tekintettel az – igazolható módon megtett – előzetes tájékoztatás nem valósítható meg másképpen, a papír alapú dokumentum bármelyik oldalán vagy az ahhoz csatolt dokumentumon fel kell tüntetni legalább az adatkezelési tájékoztató – GDPR 13. cikkében foglalt minimum követelményeknek megfelelő – kivonatát, amelyen az érintettet tájékoztatni kell az adatkezelési tájékoztató bővített változatának elérhetőségéről.

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

A Társaság az általa foglalkoztatott személyekkel az adatkezelési tájékoztatót tartalmazó utasítás közzétételével vagy az adatkezelési tájékoztató munkáltatói jogkör gyakorló részére elektronikus úton történő megküldésével közli, mindezt azzal, hogy a munkáltatói jogkörgyakorló köteles valamennyi, az irányítása alatt lévő érintett részére elektronikus úton vagy a helyben szokásos módon, igazolható formában közölni az adatkezelési tájékoztatót. A helyben szokásos módon történő tájékoztatásra vonatkozó szabályokat külön utasítás tartalmazza.

II. Az adatkezelési tájékoztató közzétételére vonatkozó kötelezettségek:

Azt az adatkezelési tájékoztatót, amely olyan adatkezelésre vonatkozik, amelyben a Társaság olyan érintett személyes adatát is kezeli, aki nem áll foglalkoztatásra irányuló jogviszonyban a Társasággal, a Társaság honlapján közzé kell tenni és annak elérhetőségét folyamatosan biztosítani kell. A közzétételről – az adatkezelési tájékoztató adatvédelmi tisztviselő által történő megküldése mellett – a Marketing és utastájékoztatás szervezeti egység gondoskodik.

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

a) az adatkezelési folyamatot szabályozó utasítás függelékeként a Társaság Utasítástárában;
b) amennyiben az adatkezelési tájékoztató nem függeléke valamely normatív szabályozónak – ideértve az átmeneti, eseti adatkezelésekre vonatkozó adatkezelési tájékoztatókat is -, úgy az Utasítástárban erre a célra kialakított felületen (menüpontban);
c) az elektronikus elérhetőséggel nem rendelkező érintettek részére a helyben szokásos módon igazolható formában;
d) az adatkezelési folyamat sajátosságait figyelembevéve az adatkezelési folyamatot szabályozó normatív szabályozásban foglalt egyéb módon

kell közzé tenni és biztosítani annak folyamatos elérhetőségét.

Helyben szokásos módon történő közzététel teljesíthető azzal, hogy a munkavállaló érintett igazolható módon tájékoztatásra kerül arról, hogy mely elektronikus elérhetőséggel rendelkező munkavállalótól kérheti az adatkezelési tájékoztató rendelkezésre bocsátását papír alapon is. E kötelezettség teljesítésében az adatvédelmi munkacsoport tagja közreműködik.

A munkaviszonyt érintő változás esetén (pl. munkáltató személyében bekövetkező változás) az ezzel összefüggésben végzett adatkezelésre vonatkozó tájékoztatást a munkaviszonyt érintő változásról történő tájékoztatással egy időben – írásban igazolható módon – kell megtenni.

III. A munkaviszony létesítésével, fenntartásával és megszűnésével (megszüntetésével) összefüggésben végzett adatkezelésekről szóló adatkezelési tájékoztatóra vonatkozó speciális rendelkezések

A 4.6.3.3. I-II. pontban foglaltaktól eltérően a Társaság a munkaviszony létesítésével, fenntartásával és megszűnésével (megszüntetésével) összefüggésben végzett adatkezelésekről szóló adatkezelési

tájékoztatójának (a továbbiakban e pont keretében: „munkavállalói adatkezelési tájékoztató”) munkavállalókkal történő közlése és részükre történő elérhetővé tétele az alábbiak szerint történik.

a) A munkavállalói adatkezelési tájékoztatót a mindenkor hatályos toborzás-kiválasztási utasításban foglaltak szerint kell az új felvételes munkavállalókkal megismertetni.

b) A munkavállalói adatkezelési tájékoztatót
   ba) az elektronikus hozzáféréssel rendelkező munkavállaló részére
   - az Utasítástár önálló menüpontjában közzé kell tenni és biztosítani kell annak folyamatos elérhetőségét, illetve
   - a MÁV Szolgáltató Központ Humánszolgáltató szervezete által kezelt intranetes felületen közzé kell tenni.

   bb) az elektronikus elérhetőséggel nem rendelkező munkavállalók részére a szolgálati felettes helyben szokásos módon – igazolható formában – teljesíti, a munkavállaló kifejezett kérésére köteles a munkavállalói adatkezelési tájékoztatót – igazolható formában – rendelkezésre bocsátani.

Amennyiben a munkavállalói adatkezelési tájékoztató módosításra kerül, úgy arról a munkavállalókat az alábbiak szerint kell tájékoztatni. A tájékoztatást megelőzően a tájékoztatás szövegét egyeztetni kell az adatvédelmi tisztviselővel.

a) Az elektronikus elérhetőséggel rendelkező munkavállalókat belső vállalati hírlevél (a továbbiakban: belső hírlevél) formájában kell tájékoztatni. A belső hírlevél a munkavállalói adatkezelési tájékoztató módosításán, illetve kifejezetten ehhez kapcsolódó kiegészítő tájékoztatáson kívül más információt nem tartalmazhat. A módosított munkavállalói adatkezelési tájékoztatót a belső hírlevélhez „pdf.” formátumban csatolni kell, vagy a belső hírlevélnek tartalmaznia kell a munkavállalói adatkezelési tájékoztató közvetlen elérhetőségét lehetővé tévő elektronikus linket. A belső hírlevélben rövid, tömör és érthető formában tájékoztatást kell adni a munkavállalói adatkezelési tájékoztatóban történt változásokról.
b) az elektronikus elérhetőséggel nem rendelkező munkavállalókat, így különösen parancskönyvi rendelkezés keretében, menetlevél kiadása során vagy más igazolható módon kell tájékoztatni, amelyhez „pdf.” formátumban csatolni kell a munkavállalói adatkezelési tájékoztatót. A parancskönyvi rendelkezés vagy menetlevél kiadása során történő tájékoztatás a munkavállalói adatkezelési tájékoztató módosításán, illetve kifejezetten ehhez kapcsolódó kiegészítő tájékoztatáson kívül más információt nem tartalmazhat. A parancskönyvi rendelkezésben vagy pl. menetlevél kiadása során meg kell jelölni azt a személyt, akitől a munkavállaló jogosult kérni a munkavállalói adatkezelési tájékoztató nyomtatott formában történő rendelkezésre bocsátását. A parancskönyvi rendelkezésben vagy menetlevél kiadása során történő átadás esetén rövid, tömör és érthető formában, igazolható módon tájékoztatást kell adni a munkavállalói adatkezelési tájékoztatóban történt változásokról.

IV. Az adatkezelési tájékoztatók nyilvántartására vonatkozó kötelezettség

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

Az adatkezelési tájékoztatót nyilvántartási számmal kell ellátni, amelynek felépítése „AT”, mint adatkezelési tájékoztató, egy „/” jel és az adatkezelési tájékoztató sorszáma négy karakterig (pl. AT/0001). Amennyiben az adatkezelési tájékoztató módosításra kerül, úgy a módosítást a módosítás sorszámának megjelölésével jelölni kell az adatkezelési tájékoztató nyilvántartási számában (pl. AT/0001-01). Amennyiben egy adatkezelési tájékoztató hatályon kívül helyezésre kerül, de ugyanazon adatkezelési folyamat keretében új adatkezelési tájékoztató kiadására kerül sor, úgy az új

adatkezelési tájékoztatónak új sorszámot kell kiosztani.. Új adatkezelési tájékoztató kiadásának kell tekinteni amennyiben az adatkezelési folyamatot szabályozó normatív szabályozó hatályon kívül helyezésre kerül és az adatkezelési folyamat tekintetében új normatív szabályozó kerül kiadásra.

4.6.3.4. Az adatbiztonsági intézkedések meghatározása

Az adatkezelő szervezeti egység az adatkezelési folyamat megtervezése során
- a tudomány és technológia állása és a megvalósítás költségei, továbbá
- az adatkezelés jellege, hatóköre, körülményei és céljai, valamint
- a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével

megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

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

Az adatbiztonsági intézkedések meghatározása során az IBSZ és a mindenkor hatályos Iratkezelési Szabályzat rendelkezéseit kell figyelembe venni. Az adatbiztonsági intézkedések meghatározása során az adatvédelmi tisztviselő mellett a Biztonsági Főigazgatóság információvédelmi szakterületének bevonása is szükséges.

4.6.4. Az adatkezelési tevékenységek nyilvántartása

Az adatvédelmi tisztviselő az adatkezelő szervezeti egységek által végzett adatkezelési folyamatokról a jelen utasításban foglalt tartalommal nyilvántartást vezet (a továbbiakban: adatkezelési tevékenységek nyilvántartása). Az adatvédelmi tisztviselő az adatkezelési tevékenységek nyilvántartásában az adatkezelő szervezeti egység által a 3. számú függelék szerinti bejelentő lap alapján, vagy saját hatáskörben történő észlelés alapján rögzíti az adatkezelési folyamatot. Az adatkezelési tevékenységek nyilvántartásában szereplő bármely adatkezelési folyamat változása, illetve új adatkezelési folyamat megkezdése esetén az adatkezelő szervezeti egység a 3. számú függelék szerinti formanyomtatvány alkalmazásával haladéktalanul köteles adatot szolgáltatni az adatvédelmi tisztviselő részére. Az adatkezelési tevékenységek nyilvántartásában szereplő információk adatvédelmi tisztviselő részére történő szolgáltatásáért az adatkezelő szervezeti egység vezetője felelős.

Az adatvédelmi tisztviselő az adatkezelési tevékenységek nyilvántartását a Társaság közös meghajtóján az adatvédelmi munkacsoport részére létrehozott mappában lévő önálló mappában vezeti, amelyhez az adatvédelmi munkacsoport tagjai olvasási jogosultsággal rendelkeznek.

Az adatkezelési tevékenységek nyilvántartásának tartalmaznia kell:

a) Az adatkezelő szervezetre vonatkozó információkat, ennek keretében:
   aa) az adatkezelő szervezet megnevezését,
   ab) a területi egység megnevezését,
   ac) az adatkezelési folyamatban esetlegesen részt vevő további adatkezelő(k), illetve adatfeldolgozó(k) megnevezését.

b) Az adatkezelési folyamatra vonatkozó információkat, ennek keretében:

ba) az adatkezelési folyamat megnevezését a tevékenység/feladat alapján, amelyhez az adatkezelés kapcsolódik,
bb) az adatkezelés célját/céljait,
bc) az adatkezelés jogalapját,
bd) az érintettek kategóriáit,
be) a kezelt személyes adatok kategóriáit,
bf) a személyes adatok forrását,
bg) az adatkezelési folyamatra irányadó jogszabály vagy belső szabályozó megjelölését,
bh) a személyes adatok megőrzésének időtartamát vagy az adatkezelés időtartamának meghatározásának szempontjait,
bi) az adatkezelési folyamatra vonatkozó adatkezelési tájékoztató meglétét, illetve annak elérhetőségét,
bj) a személyes adatok továbbítására vonatkozó információt azzal, hogy amennyiben a személyes adatok valamely címzett(ek) részére továbbításra kerülnek, úgy legalább a címzett(ek) kategóriájának megjelölése szükséges
bj) az adatkezelési tájékoztató sorszáma.

c) Az adatkezelési folyamat során alkalmazott speciális adatbiztonsági intézkedéseket, valamint a személyes adatok tárolásának módjára (elektronikus úton – ideértve az adathordozót is –, papír alapon) vonatkozó információkat. Speciális adatbiztonsági intézkedésnek minősül a jelen utasítás, valamint a mindenkor hatályos IBSZ-ben előírt adatbiztonsági intézkedésen felül alkalmazott szervezési és technikai intézkedés.

d) A személyes adatok tárolásának módját (az adathordozó típusát) és helyét.

4.6.5. Az adatvédelmi incidens kezelése

Amennyiben a Társaság bármely adatkezelő szervezeti egységénél adatvédelmi incidens következik be, úgy annak kezelésére a jelen utasításban foglaltakat kell alkalmazni. Amennyiben az adatvédelmi incidens a Társaság által adatfeldolgozói minőségben kezelt személyes adatokat érint, az adatvédelmi incidens kivizsgálására – a jelen utasításban meghatározott szabályokon túl – az adatfeldolgozási szerződésben foglaltakat kell alkalmazni. Amennyiben az adatvédelmi incidens a Társaság által közös adatkezelői minőségben kezelt személyes adatokat érint, az adatvédelmi incidens kivizsgálására – a jelen utasításban meghatározott szabályokon túl – a közös adatkezelésről szóló szerződésben foglaltakat kell alkalmazni.

4.6.5.1. Az adatvédelmi incidens kezelésére vonatkozó szabályok

Amennyiben a Társaság bármely munkavállalója észleli, hogy a Társaságnál olyan esemény történt, amely feltehetően adatvédelmi incidensnek minősül, úgy haladéktalanul, de legkésőbb 8 órán belül köteles elektronikus úton írásban az adatvedelem@mav-start.hu e-mail címen, a jelen szabályzat 11. számú függelékben található incidens bejelentő lap megküldésével, vagy az abban foglalt kötelező tartalommal, és haladéktalanul, de legkésőbb az adatvédelmi incidens gyanús esemény észlelését követő 2 órán belül telefonon tájékoztatni az adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő a telefonon kapott tájékoztatás alapján minden szükséges intézkedést megtesz az adatvédelmi incidens gyanús esemény kivizsgálásának elősegítése érdekében, és – amennyiben arra korábban nem került sor – az írásos tájékoztatást követően haladéktalanul felveszi a kapcsolatot az adatvédelmi incidenssel érintett adatkezelő szervezeti egység(ek) vezetőjével. Amennyiben az adatvédelmi incidens elektronikus úton végzett adatkezelési folyamatot érint, úgy értesíteni kell a Biztonsági Főigazgatóság információvédelmi szakterületét is.

Az adatvédelmi incidens azonosítása az előzetes vizsgálat során:

A Társaság adatvédelmi tisztviselője és az adatkezelő szervezeti egység (egységek) vezetője, valamint – a szükség esetén bevont – információvédelmi szakértő előzetes vizsgálatot folytat le annak érdekében, hogy megállapításra kerüljön adatvédelmi incidens következett-e be. Az előzetes vizsgálatról feljegyzést kell készíteni, amelyben rögzíteni kell:

- az incidensre vonatkozó körülményeket (kitérve arra is, hogy az incidens érinti-e a Társaság által alkalmazott bármely informatikai rendszert, illetve fennáll-e az esélye az érintettek szélesebb körének személyes adatainak szivárgására, jogosulatlan személyek általi hozzáférésre),
- a vizsgálat időpontját,
- a vizsgálat helyét,
- a vizsgálatban résztvevő személyek nevét, munkakörét és
- annak megállapítását, hogy adatvédelmi incidens történt-e és azt, hogy milyen körülmények támasztják alá az adatvédelmi incidens bekövetkezését.

Amennyiben az előzetes vizsgálat során megállapításra kerül, hogy nem következett be adatvédelmi incidens, a vizsgálat lezárható. Amennyiben az előzetes vizsgálat alapján megállapításra kerül, hogy adatvédelmi incidens következett be, úgy az adatvédelmi incidenst részletesen ki kell vizsgálni, és ilyen esetben az adatvédelmi incidens gyanús esemény előzetes vizsgálatáról feljegyzés készítése nem szükséges, az előzetes vizsgálatra vonatkozó megállapításokat az adatvédelmi incidens vizsgálatáról készült jelentés tartalmazza. Amennyiben az előzetes vizsgálat során nem állapítható meg egyértelműen, hogy adatvédelmi incidens következett-e be, úgy – az adatvédelmi incidens kivizsgálására vonatkozó szabályok alkalmazása mellett – a vizsgálatot tovább kell folytatni.

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

Amennyiben az adatvédelmi incidens olyan személyes adatokat érint, amelyeket a Társaság adatfeldolgozóként kezel, úgy – az adatfeldolgozási szerződésben foglaltaknak megfelelően – értesíteni szükséges az e személyes adatok tekintetében adatkezelőnek minősülő szerződött partnert is.

Az adatvédelmi incidens kivizsgálása:

Az adatvédelmi incidens kivizsgálása céljából az adatvédelmi tisztviselő vizsgálóbizottságot alakít. A vizsgálóbizottságot úgy kell kialakítani, hogy az adatvédelmi incidens kivizsgálása akadálymentesen és határidőben megvalósuljon. A vizsgálóbizottság tagja:

a) az adatvédelmi tisztviselő,
b) az adatvédelmi incidenssel érintett adatkezelő szervezeti egység(ek) vezetője (vezetői),
c) amennyiben az adatvédelmi incidens elektronikus úton végzett adatkezelést érint, úgy a Biztonsági Főigazgatóság információvédelmi szakértője,
d) amennyiben az adatvédelmi incidens informatikai rendszert érint, a Digitális Igazgatóság Rendszermenedzsment szervezet vezetője, vagy az általa kijelölt személy,
e) amennyiben az adatvédelmi incidens a Társaság munkavállalóinak személyes adatait érinti, úgy a humánerőforrás főigazgató által kijelölt munkavállaló,
f) az adatvédelmi incidens jellegétől függően szükség szerint más szakterület vezetője vagy az általa kijelölt személy,
g) amennyiben az adatvédelmi incidens olyan személyes adatot érint, amelynek kezelése során az adatkezelő szervezeti egység adatfeldolgozót vesz igénybe, úgy az adatfeldolgozó által kijelölt személy.

A vizsgáló bizottság az adatvédelmi incidens körülményeinek kivizsgálása során meghatározza az adatvédelmi incidens jellegét, az adatvédelmi incidensben érintett személyek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,

az adatvédelmi incidens ismert és valószínűsíthető következményeit, továbbá az adatvédelmi incidens orvoslása, illetve további következményeinek elkerülése érdekében már megtett intézkedéseket.

Az adatvédelmi incidenseket típusuk szerint különösen az alábbi kategóriákba sorolhatjuk:
- Bizalmassági incidens: személyes adatok véletlen vagy felhatalmazás nélküli közlése vagy az ezekhez való jogosulatlan hozzáférés. A bizalmassági incidenst bekövetkezettnek kell tekinteni abban az esetben is, ha a személyes adatokhoz való jogosulatlan hozzáférés lehetősége fennáll, de az adatvédelmi incidens körülményeinél fogva nem igazolható a személyes adatokhoz arra nem jogosult személyek által történő tényleges hozzáférés.
- Sértetlenséggel kapcsolatos incidens: személyes adatok véletlen vagy jogosulatlan megváltoztatása.
- Hozzáférhetőséggel kapcsolatos incidens: személyes adatok véletlen vagy jogosulatlan megsemmisítése vagy a személyes adatok elvesztése.

Az adatvédelmi incidens körülményeinek meghatározását követően a vizsgáló bizottság értékeli az adatvédelmi incidens valószínűsíthető kockázatait. A kockázatelemzés célja, hogy a Társaság értékelje azt, hogy az adatvédelmi incidens milyen hatással van, illetve lehet az érintettek jogaira és szabadságaira. Az adatvédelmi incidens kockázati besorolása az alábbi lehet:
a) nincs kockázat,
b) van kockázat,
c) magas kockázat.

Az adatvédelmi incidens kockázatelemzése, értékelése alapján kell meghatározni az adatvédelmi incidens következményeinek elhárításához szükséges intézkedéseket, valamint azt, hogy a Társaságot terheli-e az adatvédelmi incidens bejelentésére vonatkozó kötelezettség, illetve arról értesíteni kell-e az érintetteket. Az adatvédelmi incidens kockázatainak értékelését az adatvédelmi incidens bekövetkezését követő 70 órán belül legalább olyan szinten el kell végezni, hogy abból megállapítható legyen, hogy az adatvédelmi incidenst be kell-e jelenteni az adatvédelmi hatóság részére. Az adatvédelmi incidens vizsgálatáról a 12. számú függelék szerinti összefoglaló jelentést kell készíteni.

Amennyiben az adatkezelő szervezeti egység az adatvédelmi incidenssel érintett adatkezelési folyamat tekintetében már végzett hatásvizsgálatot, amelyben felmérte egy potenciális adatvédelmi incidens során felmerülő kockázatokat, úgy ennek figyelembevételével és felhasználásával kell a kockázatelemzést elvégezni.

A kockázatelemzést az alábbi szempontok szerint kell elvégezni:
- az incidens típusa,
- a személyes adatok típusa (különleges és/vagy nem különleges adat),
- a személyes adatok száma (külön meghatározva a különleges adatok számát),
- a személyes adatok köre,
- lehetséges-e az érintettek azonosítása, ha igen, az könnyen megvalósulhat-e,
- milyen következményei vannak, illetve lehetnek az incidensnek az érintettre nézve és a következményeknek milyen súlya van, illetve lehet,
- az adatvédelmi incidensben érintett személyek kategóriái, külön megjelölve az érintett személyek speciális kategóriáit,
- az érintettek száma (külön meghatározva a speciális érintettek számát),
- az adatvédelmi incidens társadalomra vagy az érintettek nagyobb csoportjára gyakorolt hatása.

A természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázatúnak kell tekinteni az adatvédelmi incidenst, ha az különleges adatokat, az érintett pénzügyi helyzetével

összefüggő adatokat – ideértve a banki adatokat is –, az érintett társadalmi megbecsülésére kiható adatokat, az érintett által alkalmazott felhasználónevet és jelszót, a személyiséglopásra alkalmas adatokat érint, valamint, ha igazolt, hogy az érintettet pénzügyi veszteség érte az adatvédelmi incidens miatt. Valószínűsíthetően magas kockázatúnak kell tekinteni az adatvédelmi incidenst továbbá akkor is, ha az incidensben érintett személyes adatok száma vagy az érintettek száma meghaladja az ötvenet, vagy az incidensben 16. életévet be nem töltött személyek is érintettek.

Az adatvédelmi incidens értékelésének további követelményeit a 14. számú függelék tartalmazza.

Az adatvédelmi incidenssel kapcsolatos jelentés és intézkedési terv

A vizsgálóbizottság az adatvédelmi incidens kivizsgálásáról jelentést készít, amelyben meghatározza az adatvédelmi incidens következményeinek elhárításához vagy enyhítéséhez, valamint a további adatvédelmi incidens bekövetkezésének elkerüléséhez szükséges intézkedéseket, megjelölve az intézkedés végrehajtásáért felelős szervezeti egységet és a végrehajtás határidejét. Az adatvédelmi incidens kivizsgálásáról szóló jelentést és az intézkedési tervet jóváhagyásra meg kell küldeni a Társaság vezérigazgatójának.

Az intézkedési terv végrehajtásáért felelős szervezeti egység az intézkedési terv végrehajtására nyitva álló határidőt követő 15 napon belül írásos jelentést készít az intézkedési terv végrehajtásának eredményéről. A jelentést meg kell küldeni az adatvédelmi tisztviselő részére, aki azt véleményezésre megküldi az intézkedési terv készítésében részt vevő vizsgálóbizottsági tagok részére. Az intézkedési terv végrehajtásának eredményéről az adatvédelmi tisztviselő a jelentés kézhezvételét követő 15 napon belül beszámol a Társaság vezérigazgatójának, amelyben ismertetni kell a vizsgálóbizottság tagjainak véleményét is.

Az adatvédelmi incidens bejelentése az adatvédelmi hatóság részére

A vizsgálóbizottság a jelentésben javaslatot tesz arra vonatkozóan, hogy az adatvédelmi incidenst be kell-e jelenteni a NAIH részére. Az adatvédelmi hatóságnak történő bejelentés szükségességéről a Társaság vezérigazgatója dönt. Amennyiben az adatvédelmi incidens NAIH részére történő bejelentéséről dönt a Társaság vezérigazgatója, úgy az adatvédelmi incidenst az adatvédelmi tisztviselő indokolatlan késedelem nélkül, de legkésőbb az adatvédelmi incidens tudomásra jutásától számított 72 órán belül bejelenti a NAIH részére, ha az adatvédelmi incidens valószínűsíthetően kockázattal jár az érintettek jogaira és szabadságaira nézve. Tudomásszerzésnek minősül az az időpont, amelyben az esetleges adatvédelmi incidens előzetes vizsgálata során megállapításra kerül az adatvédelmi incidens bekövetkezése.

Az adatvédelmi incidenst a NAIH részére elektronikus úton az adatvédelmi hatóság honlapján az incidens bejelentése céljából közzétett, rendszeresített formanyomtatványon kell bejelenteni. Amennyiben az adatvédelmi incidens bejelentésekor nem áll rendelkezésre valamennyi információ, úgy az első bejelentéskor a rendelkezésre álló információkat szükséges bejelenteni, majd a többi adatot azok rendelkezésre állását követően indokolatlan késedelem nélkül kell a NAIH részére megküldeni, megjelölve a késedelem igazolására szolgáló indokokat.

Az első bejelentés alkalmával legalább az alábbi adatokat szükséges megadni a NAIH részére:
- az adatvédelmi incidens jellege,
- az adatvédelmi incidensben érintettek kategóriái és hozzávetőleges száma,
- az adatvédelmi incidensben érintett személyes adatok kategóriái és – legalább hozzávetőleges száma,
- az adatvédelmi tisztviselő neve, elérhetősége,
- az adatvédelmi incidensből eredő, valószínűsíthető következmények,

- az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintettek tájékoztatása az adatvédelmi incidensről

A vizsgálóbizottság a jelentésben javaslatot tesz arra vonatkozóan, hogy az adatvédelmi incidensről szükséges-e tájékoztatni az érintette(ke)t, egyúttal szövegjavaslatot tesz az érintettek tájékoztatásához kapcsolódóan és javaslatot tesz az érintettek tájékoztatásának módjáról, formájáról. Az érintett(ek) tájékoztatásának szükségességéről, módjáról és szövegéről a Társaság vezérigazgatója dönt. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő szervezeti egység – az adatvédelmi tisztviselő közreműködésével – indokolatlan késedelem nélkül tájékoztatja az érintetteket az adatvédelmi incidensről, amely tájékoztatásban ismertetnie kell az adatvédelmi incidens jellegét, következményeit, az adatvédelmi incidens következményeinek elhárítására tett intézkedéseket, valamint közölni kell az adatvédelmi tisztviselő elérhetőségét.

Nem kell tájékoztatni az érintetteket, ha:
- a személyes adatok tárolása olyan titkosított módszerrel történt, amely miatt a személyes adatok harmadik személyek számára nem értelmezhetők,
- az adatkezelő olyan hatékony intézkedést tett az adatvédelmi incidens következményeinek elhárítására, amelyek eredményeként a magas kockázat a továbbiakban valószínűsíthetően nem valósul meg,
- aránytalan erőfeszítés lenne az érintettek közvetlen tájékoztatása, ebben az esetben a Társaság közleményt adhat ki a bekövetkezett adatvédelmi incidensről.

Amennyiben az adatvédelmi incidensben az érintettekkel való kapcsolattartást lehetővé tevő csatorna érintett, úgy az érintettek tájékoztatására ez a csatorna nem alkalmazható. Amennyiben annak feltételei rendelkezésre állnak, az érintetteket az alábbi kommunikációs csatornákon lehet tájékoztatni: postai levélben, elektronikus levélben (e-mail), SMS-ben, a Társaság honlapján, sajtóközleményben.

Az incidensről szóló tájékoztatás egyértelmű és átlátható jellegének biztosítása érdekében az nem küldhető ki más jellegű tájékoztatással együtt.

4.6.5.2. Korrekciós intézkedések

Az adatvédelmi incidens vizsgálatát végző vizsgálóbizottság az adatvédelmi incidens vizsgálatáról szóló jelentésben, vagy az adatvédelmi tisztviselő önállóan az adatvédelmi incidenst követően szükség esetén állásfoglalást bocsát ki arról, hogy az adatkezelő szervezeti egység(ek)nek milyen további intézkedés(ek) megtételét javasolja az adatvédelmi incidens(ek) megelőzése érdekében.

Ilyen intézkedés lehet:
- az adatkezelési folyamatra irányadó szabályozás felülvizsgálata, szükség szerinti módosítása, vagy annak hiányában szabályozás kialakítása,
- az adatkezelési folyamatra irányadó szabályozás betartásának fokozott ellenőrzése,
- képzések, oktatások szervezése, ideértve a múltban bekövetkezett adatvédelmi incidensek tapasztalatainak összegzését is.

Az adatvédelmi tisztviselő korrekciós intézkedésre vonatkozó állásfoglalását megküldi az adatkezelő szervezeti egység vezetőjének. A korrekciós intézkedés végrehajtásáról az adatkezelő szervezeti egység tájékoztatja az adatvédelmi tisztviselőt.

4.6.5.3. Az adatvédelmi incidens kezelésének lezárása

Az adatvédelmi tisztviselő az adatvédelmi incidens kezelésének folyamatát az intézkedési terv vagy – amennyiben korrekciós intézkedés megtételére került sor – a korrekciós intézkedés végrehajtásáról szóló tájékoztatás kézhezvételét követően lezárja és erről feljegyzést készít. Az adatvédelmi incidens kezelési folyamatának lezárásáról az adatvédelmi tisztviselő tájékoztatja a Társaság vezérigazgatóját.

4.6.5.4. Az adatvédelmi incidens nyilvántartása

Az adatvédelmi tisztviselő a 13. számú függelék szerinti tartalommal nyilvántartja az adatvédelmi incidenseket.

4.6.5.5. Az egyes adatvédelmi incidensekre vonatkozó eltérő rendelkezések

Amennyiben az adatvédelmi incidens a Társaság tulajdonában álló szolgálati IT eszköz (telefon, laptop, tablet; a továbbiakban: IT eszköz) munkavállaló birtokából való kikerülésében nyilvánul meg, úgy az ilyen módon bekövetkezett adatvédelmi incidens kivizsgálására – a 4.6.5.1 – 4.6.5.3. pontokban foglaltak mellőzése mellett – a jelen alpontban foglalt eltérésekkel kell alkalmazni.

Az IT eszköz munkavállaló birtokából való kikerülését a munkavállaló köteles a külön utasításban foglaltak szerint – az erre a célra kialakított SharePoint alapon működő bejelentő felületen – bejelenteni és a bejelentő felületen kötelezően megválaszolandó kérdésként megjelölt kérdéseket megválaszolni (a továbbiakban a jelen pont keretében: bejelentés). A bejelentésben megadott információk alapján az adatvédelmi tisztviselő – szükség szerint az információvédelmi szakértő bevonásával – felméri és megvizsgálja az IT eszköz munkavállaló birtokából való kikerülésének kockázatait. Amennyiben a bejelentésben foglaltak alapján nem állapítható meg az, hogy az IT eszköz munkavállaló birtokából történő kikerülésének milyen kockázata(i) van(nak), úgy az adatvédelmi tisztviselő írásban (e-mailben) felhívja a bejelentőt a bejelentésének kiegészítésére, további információk szolgáltatására, illetve felszólítja az adatvédelmi incidens ismert következményeinek orvoslása, illetve a lehetséges következményeinek megelőzése érdekében megtenni szükséges intézkedések végrehajtására. A munkavállaló a megkeresésre 1 munkanapon belül köteles választ adni.

Amennyiben a bejelentésben foglaltak alapján megállapításra kerül, hogy az IT eszköz munkavállaló birtokából való kikerülésének kockázata(i) van(nak), úgy a vizsgálatot a jelen fejezetben foglaltaknak megfelelően el kell végezni.

A jelen alpontban foglaltak szerint bekövetkezett adatvédelmi incidensre vonatkozó vizsgálat eredményét a bejelentés megtételére szolgáló SharePoint felületen erre a célra kialakított helyen kell rögzíteni. A jelen alpont szerinti adatvédelmi incidens kivizsgálásával összefüggésben a személyes adatokon végzett adatkezelésre vonatkozó adatkezelési tájékoztatást a bejelentés megtételére szolgáló SharePoint felületen kell teljesíteni.

A jelen alpontban foglaltak szerint bekövetkezett és kivizsgált adatvédelmi incidensek nyilvántartása a bejelentő felülethez tartozó SharePoint felületen történik. A jelen alpontban foglaltak szerint bekövetkezett és kivizsgált adatvédelmi incidensekről az éves beszámolóban kell tájékoztatást nyújtani a Társaság vezérigazgatója részére.

4.6.6. A személyes adatok továbbításával kapcsolatos rendelkezések

A jelen fejezetben foglalt szabályokat a személyes adatokat tartalmazó papír alapon rögzített vagy elektronikusan tárolt dokumentumok tekintetében a mindenkor hatályos Iratkezelési Szabályzattal összhangban és annak eltérő rendelkezése hiányában kell alkalmazni.

A jelen fejezetben foglalt szabályokat az elektronikus úton végzett adattovábbítás tekintetében a mindenkor hatályos IBSZ-ben foglaltakkal összhangban és annak eltérő rendelkezése hiányában kell alkalmazni.

4.6.6.1. A személyes adatok Társaságon belüli továbbítása

A személyes adato(ka)t tartalmazó elektronikus dokumentumok Társaságon belüli továbbításának módját és az alkalmazandó adatbiztonsági intézkedéseket (pl. szükséges e jelszóvédelem) – a továbbítandó személyes adatok jellegének és számának, valamint az érintettek számának és kategóriájának figyelembevételével – az adattovábbítással érintett adatkezelési folyamatot szabályozó belső normatív szabályozóban kell meghatározni, amely során törekedni kell arra, hogy a személyes adatok továbbítását

a) elsősorban a Társaság közös meghajtóján kifejezetten a személyes adatok rendelkezésre bocsátása céljából létrehozott – korlátozott hozzáférésű – mappában,
b) amennyiben az a) pontban foglaltak végrehajtása nem lehetséges vagy az adatkezelés jellegét tekintve aránytalan nehézségekkel jár, úgy a Társaság által alkalmazott SharePoint felületen,
c) amennyiben a b) pontban foglaltak végrehajtása nem lehetséges vagy az adatkezelés jellegét tekintve aránytalan nehézségekkel jár, úgy – a d) pontban foglaltakon kívüli – a személyes adatok továbbítását lehetővé tévő, adatbiztonsági szempontból is megfelelő más módszer alkalmazásával,
d) elektronikus levélben, annak csatolmányaként történő megküldésével

kell végrehajtani.

Amennyiben az adattovábbítás a d) pontban foglaltak szerint történik és a továbbítandó elektronikus dokumentum különleges adatot tartalmaz (pl. egészségügyi adat), úgy azt – az IBSZ-ben foglaltaknak megfelelően képzett – jelszóval kell védeni és a jelszót a címzett részére SMS-ben vagy külön e-mailben kell rendelkezésre bocsátani.

Amennyiben a személyes adatot tartalmazó dokumentum továbbítása külső adathordozón történik meg, úgy – az adathordozó tekintetében az IBSZ-ben előírt adatbiztonsági követelményeken túl – a külső adathordozót titkosítani szükséges és a személyes adatot tartalmazó dokumentum tekintetében alkalmazandó további adatbiztonsági intézkedést (pl. jelszóvédelem) az adattovábbítással érintett adatkezelési folyamatot szabályozó belső normatív szabályozóban kell meghatározni.

A személyes adato(ka)t tartalmazó – papír alapon vagy elektronikusan kezelt – dokumentumok Társaságon belüli továbbítása során az adattovábbítást végző szervezeti egység felelős azért, hogy az a munkavállaló, aki a személyes adato(ka)t tartalmazó dokumentumot megkapja, jogosult legyen a személyes adatok megismerésére és kezelésére. Amennyiben az adattovábbítás eredményeként a személyes adato(ka)t tartalmazó dokumentumot megismerő munkavállaló észleli, hogy a személyes adatok megismerésére nem jogosult (a továbbiakban e pont keretében: téves belső adattovábbítás), úgy haladéktalanul köteles ezt jelezni a szolgálati felettesének, illetve a téves belső adattovábbítást végző munkavállalónak, illetve e munkavállaló szolgálati felettesének. A téves belső adattovábbítást végző munkavállaló és annak címzettje egyaránt köteles – a munkáltatói jogkörgyakorló tájékoztatása mellett – bejelenteni a téves belső adattovábbítást az adatvédelmi tisztviselő részére – a jelen utasítás 4.6.5.1. pontjában foglaltaknak megfelelően. Amennyiben a bejelentést bármely munkavállaló elmulasztja, úgy a bejelentést a munkáltatói jogkörgyakorló köteles megtenni, feltéve, hogy a téves belső adattovábbításról tudomással bír.

4.6.6.2. A személyes adatok Társaságon kívül történő továbbítása

A személyes adato(ka)t tartalmazó elektronikus dokumentumok Társaságon kívüli továbbításának módját és az alkalmazandó adatbiztonsági intézkedéseket (pl. szükséges e jelszóvédelem) – a továbbítandó személyes adatok jellegének és számának, valamint az érintettek számának és kategóriájának figyelembevételével – az adattovábbítással érintett adatkezelési folyamatot

szabályozó belső normatív szabályozóban vagy – amennyiben ilyen van – a címzettel kötött szerződésben kell meghatározni, amely során törekedni kell arra, hogy a személyes adatok továbbítását

a) elsősorban a Társaság által alkalmazott SharePoint felületen,
b) a Címzett által alkalmazott/üzemeltetett olyan felületen vagy rendszerben történjen, amelyhez a Címzett biztosítja a hozzáférést a Társaság részére,
c) amennyiben az a) vagy b) pontban foglaltak végrehajtása nem lehetséges vagy az adatkezelés jellegét tekintve aránytalan nehézségekkel jár, úgy – a d) pontban foglaltakon kívüli – a személyes adatok továbbítását lehetővé tévő, adatbiztonsági szempontból is megfelelő más módszer alkalmazásával,
d) elektronikus levélben, annak csatolmányaként történő megküldésével

kell végrehajtani.

Amennyiben az adattovábbítás a d) pontban foglaltak szerint történik és a továbbítandó elektronikus dokumentum különleges adatot tartalmaz (pl. egészségügyi adat), úgy azt – az IBSZ-ben foglaltaknak megfelelően képzett – jelszóval kell védeni és a jelszót a címzett részére a személyes adatok megküldésére alkalmazott csatornán kell rendelkezésre bocsátani.

Amennyiben a személyes adatot tartalmazó dokumentum továbbítása külső adathordozón történik meg, úgy – az adathordozó tekintetében az IBSZ-ben előírt adatbiztonsági követelményeken túl – a külső adathordozót titkosítani szükséges és a személyes adatot tartalmazó dokumentum tekintetében alkalmazandó további adatbiztonsági intézkedést (pl. jelszóvédelem) az adattovábbítással érintett adatkezelési folyamatot szabályozó belső normatív szabályozóban kell meghatározni.

4.6.6.3. A személyes adatok harmadik országba vagy nemzetközi szervezetek részére történő továbbítása

A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó szabályokat az adatkezelési folyamatot szabályozó utasításban, a GDPR 44 – 49. cikkében foglalt rendelkezések figyelembevételével kell meghatározni.

4.6.6.4. Az egyedi adattovábbítások nyilvántartása

Az adatkezelő szervezeti egységei a valamely konkrét adatkezelési folyamathoz nem kapcsolódó egyedi adattovábbításokat kötelesek a 17. számú függelék szerinti nyilvántartásban (a továbbiakban: egyedi adattovábbítási nyilvántartás) rögzíteni és megőrizni. Az adatkezelő szervezeti egység az adatvédelmi tisztviselő erre irányuló felhívására, de legalább félévente köteles megküldeni az egyedi adattovábbítási nyilvántartást az adatvédelmi tisztviselő részére. Az adatvédelmi tisztviselő az egyedi adattovábbításokkal kapcsolatosan tájékoztatást kérhet, nem megfelelőség észlelése esetén adatvédelmi megfelelőségi vizsgálatot kezdeményezhet.

4.6.7. A személyes adatokat tartalmazó nyilvántartáshoz való hozzáférés szabályai

A jelen pontban foglalt szabályokat az IBSZ-ben foglaltakkal összhangban kell értelmezni és alkalmazni.

A személyes adatokat tartalmazó nyilvántartásokhoz – ideértve a nyilvántartást tartalmazó rendszereket, illetve egy rendszer valamely alrendszerét – való hozzáférés szabályait – ideértve a hozzáférési jogosultság formáját és korlátjait – a személyes adatok kezelésével érintett adatkezelési folyamatot szabályozó belső normatív szabályozóban kell meghatározni. A személyes adatokhoz való hozzáférési jogosultságokat úgy kell kialakítani, hogy lehetőség szerint kizárólag az adatkezelési tevékenységet végző szervezet(ek) részéről az adott folyamatban közreműködő, feladatot végző munkavállalók – és szükség esetén az adatkezelési tevékenységet végző szervezeti egység(ek) vezetői – rendelkezzenek hozzáférési joggal.

A személyes adatot tartalmazó nyilvántartáshoz történő hozzáférési jogosultság olyan személy részére történő biztosításához, aki az adatkezelési folyamat alapján hozzáférésre nem jogosult személynek minősül kizárólag akkor biztosítható, ha

a) a hozzáférési jogosultság biztosítása a Társasággal kötött megállapodás alapján fennálló kötelezettségeinek teljesítéséhez szükséges,
b) – az a) pontban foglaltak hiányában – a hozzáférési jogosultság biztosítását az adatkezelési folyamatot végző szervezeti egység(ek) vezetője, illetve vezetői írásban – ideértve az elektronikus utat (e-mail) is – jóváhagyta, illetve jóváhagyták. Ebben az esetben a személyes adatokhoz való hozzáférés biztosításával együtt járó adatkezelési kockázatot az adatkezelési folyamatot végző szervezeti egység(ek) vezetője, illetve vezetői viselik.

Amennyiben valamely személyes adatot is tartalmazó nyilvántartásból a nyilvántartáshoz hozzáféréssel nem rendelkező szervezet/személy eseti jelleggel adatszolgáltatást igényel, úgy az adatszolgáltatás nem teljesíthető a nyilvántartáshoz való hozzáférés biztosításával. Amennyiben az adatszolgáltatás teljesítéséhez a személyes adatok szolgáltatása nem szükséges, úgy a nyilvántartásban szereplő személyes adatok nem továbbíthatók, amelyhez szükség esetén a nyilvántartásról anonimizált másolatot kell készíteni. Amennyiben a személyes adatok továbbítása szükséges az adatszolgáltatás teljesítéséhez, úgy az csak akkor és annyiban lehetséges, amennyiben a személyes adatok jogszerű továbbításának feltételei fennállnak. A személyes adatok továbbítása tekintetében a 4.6.6. pont rendelkezéseit alkalmazni kell.

4.7. Az adatvédelmi megfelelőség ellenőrzése

4.7.1. Az adatvédelmi megfelelőségi vizsgálat tárgya

Az adatvédelmi tisztviselő adatvédelmi megfelelőségi vizsgálat (a továbbiakban: vizsgálat vagy audit) keretében ellenőrzi a Társaság által végzett egyes adatkezelési folyamatok adatvédelmi szabályoknak való megfelelőségét. Egy audit tárgya egy adatkezelési folyamat lehet, kivéve, ha több adatkezelési folyamat olyan mértékben függ össze, hogy a vizsgálat kizárólag az egyik adatkezelési folyamat tekintetében nem végezhető el.

A vizsgálat lefolytatására a Társaságon kívüli személy (pl. ügyvédi iroda vagy kifejezetten ilyen tevékenységet végző gazdasági társaság) részére is adható megbízás. E megbízás tekintetében a jelen utasítás és különösen a jelen fejezet szabályait megfelelően alkalmazni kell. A Társaságon kívüli személy által végzett vizsgálat lefolytatásába közreműködőként az adatvédelmi tisztviselőt be kell vonni.

4.7.2. Az adatvédelmi megfelelőségi vizsgálat elrendelése

Az adatvédelmi megfelelőségi vizsgálat lefolytatása:

a) az éves auditálási tervben foglaltak;
b) eseti elrendelés;
c) az adatvédelmi tisztviselő saját hatáskörben történő elrendelése

alapján lehetséges.

4.7.2.1. Az éves auditálási terv alapján végzett adatvédelmi megfelelőségi vizsgálat

Az adatvédelmi tisztviselő minden év december 15. napjáig elkészíti és a vezérigazgató részére jóváhagyás céljából megküldi a következő tárgyévre vonatkozó auditálási tervet. Az auditálási tervben meg kell jelölni a tárgyévben adatvédelmi vizsgálat alá vonni kívánt adatkezelési folyamatokat, úgy, hogy negyedévente legalább egy adatkezelési folyamat vizsgálatát ki kell jelölni. Az auditálási tervben vizsgálat alá vonni kívánt adatkezelési folyamatok között legalább egy adatkezelési folyamatnak – a Társaság személyszállítási szolgáltatásával összefüggésben – az utasok

személyes adatain végzett adatkezelésre, míg legalább egy adatkezelési folyamatnak a munkavállalókat érintően végzett adatkezelésre kell vonatkoznia.

A vezérigazgató az előterjesztett auditálási tervet jóváhagyja vagy módosítás, illetve kiegészítés céljából – megjelölve a módosításra, illetve kiegészítésre nyitva álló határidőt – visszaküldi az adatvédelmi tisztviselő részére. Az auditálási terv módosított, illetve kiegészített változatát ismételten meg kell küldeni a vezérigazgató részére jóváhagyás céljából. Az auditálási terv jóváhagyása esetén annak végrehajtásáról az adatvédelmi tisztviselő gondoskodik. Az auditálási terv alapján lefolytatott vizsgálat megkezdését megelőzően az auditálással érintett szervezeti egység vezetőjét tájékoztatni kell az auditálás tényéről, az auditálás tárgyáról, az auditálás idejéről (kezdő és tervezett záró időpontjáról), valamint az auditálás lefolytatásának tervezett módjáról.

Az auditálási terv alapján lefolytatott vizsgálatok tekintetében a jelen fejezet szabályait megfelelően alkalmazni kell azzal, hogy az auditálási terv vezérigazgató által történt jóváhagyása esetén nincs szükség a 2. számú függelék szerinti megbízólevél kibocsátására.

4.7.2.2. Az adatvédelmi megfelelőségi vizsgálat eseti elrendelése

A vizsgálat eseti elrendelésére jogosult
a) a vezérigazgató a Társaság bármely adatkezelő szervezeti egysége,
b) a vezérigazgató-helyettes és az igazgató az általa felügyelt adatkezelő szervezeti egységek,
c) a szervezeti egység vezetője az általa vezetett adatkezelő szervezeti egység
által végzett adatkezelési folyamat tekintetében.

Az audit elvégzésére vonatkozó megbízást az audit elrendelésére jogosult személy a 2. számú függelék szerinti megbízólevél megfelelő kitöltésével és az adatvédelmi tisztviselő részére történő megküldésével rendelheti el. Az audit elrendelését követően, a vizsgálat elrendeléséről – a vizsgálat elvégzésére vonatkozó megbízólevél megküldésével együtt – az adatvédelmi tisztviselő a Társaság vezérigazgatóját haladéktalanul, de legkésőbb a megbízólevél kézhezvételét követő két munkanapon belül tájékoztatja.

Az audit elrendelésére az adatvédelmi tisztviselő javaslatot tehet a vezérigazgató részére. Az adatvédelmi tisztviselő a javaslatában megjelöli az audit elrendelésére okot adó körülményt, az adatkezelési folyamatot és a vizsgálat elmaradásának lehetséges következményeit. Nem szükséges a 2. számú függelék szerinti megbízólevél kiállítása, ha az adatvédelmi megfelelőségi vizsgálat eseti elrendelésére egy adatvédelmi incidens miatt hozott korrekciós intézkedésként kerül sor.

Az audit lefolytatására ésszerű határidőt kell meghatározni, amelynél figyelembe kell venni különösen az adatkezelési folyamat összetettségét és a folyamatban lévő más vizsgálatokat. Az audit lefolytatására legalább 45 napot szükséges biztosítani. Az adatvédelmi tisztviselő negyedévente – ide nem értve az éves auditálási terv szerint lefolytatott vizsgálatot – összesen legfeljebb három vizsgálat lefolytatásával bízható meg.

4.7.2.3. Az adatvédelmi tisztviselő által saját hatáskörben lefolytatott adatvédelmi megfelelőségi vizsgálat

Az adatvédelmi tisztviselő saját hatáskörben vizsgálatot folytathat le
a) ha a munkavégzése során olyan adatkezelést tapasztal, amellyel kapcsolatosan felmerül a jogszerűtlen adatkezelés gyanúja;
b) bármely olyan adatkezelési folyamat tekintetében, amelynek keretében különleges adat kezelése is történik;
c) bármely olyan adatkezelési folyamat tekintetében, amelyben automatizált döntéshozatalra kerül sor;

d) azon adatkezelési folyamatok esetén, amely – az adatkezelési folyamat kockázatelemzése során – magas kockázati minősítést kapott;
e) valamely folyamatot érintően előterjesztett érintetti kérelem vagy adatvédelmi panasz teljesítése során feltárt nem megfelelőség esetén.

A vizsgálatról – a vizsgálat okának megjelölésével – a vizsgálattal érintett adatkezelési folyamatért felelős szervezeti egység vezetőjét, valamint a Társaság vezérigazgatóját előzetesen tájékoztatni kell. A vizsgálat lefolytatására a jelen fejezet szabályait megfelelően alkalmazni kell. A vizsgálatot ésszerű határidőn belül, de legfeljebb a vizsgálatról szóló tájékoztatás megküldését követő 30 napon belül le kell folytatni, a vizsgálati határidő meghosszabbítására nincs lehetőség.

4.7.3. Az adatvédelmi megfelelőségi vizsgálat lefolytatása

Az Adatkezelő szervezeti egység a vizsgálat lefolytatása során köteles együttműködni az adatvédelmi tisztviselővel. Az adatvédelmi tisztviselő a vizsgálat lefolytatása céljából betekinthet bármely személyes adatot tartalmazó vagy az adatkezeléssel érintett papír alapú és elektronikus iratba, nyilvántartásba és elektronikus rendszerbe, továbbá felvilágosítást és információt kérhet a vizsgálat alá vont adatkezelési folyamatban közreműködő munkavállalóktól.

Amennyiben a vizsgálat során felmerült körülmények indokolják, a vizsgálat lefolytatásának határideje egy alkalommal 30 nappal meghosszabbítható.

A vizsgálati határidő meghosszabbítása
a) a 4.7.2.1. pontban foglaltak alapján lefolytatott vizsgálat esetén az adatvédelmi tisztviselő által a Társaság vezérigazgatója részére a vizsgálati határidő lejártát megelőzően legalább 15 nappal előterjesztett és jóváhagyott kérelem alapján lehetséges; vagy

b) a 4.7.2.2. pontban foglaltak alapján lefolytatott vizsgálat esetén az adatvédelmi tisztviselő a vizsgálatot elrendelő személy részére terjeszti elő, amelyben meg kell jelölni a határidő meghosszabbítását indokoló körülményeket.

A határidő meghosszabbítására irányuló kérelemről a kérelem előterjesztését követő három napon belül döntést kell hozni.

4.7.4. Az adatvédelmi vizsgálat befejezése

Az adatvédelmi tisztviselő a vizsgálat elvégzését követően 15 napon belül összefoglaló jelentést (a továbbiakban: összefoglaló jelentés) készít, amely tartalmazza a vizsgált adatkezelési folyamat adatvédelmi megfelelősége tekintetében tett megállapításokat, továbbá a feltárt nem megfelelőségek kockázatait, lehetséges jogkövetkezményeit. A feltárt nem megfelelőségek kiküszöbölésére intézkedési tervet (a továbbiakban: intézkedési terv) kell készíteni.

Az összefoglaló jelentés és az intézkedési terv tervezetét (a továbbiakban e bekezdés keretében együtt: tervezet) meg kell küldeni a vizsgálattal érintett szakterület(ek) vezetőjének és a szakterület részéről kijelölt vizsgálatban közreműködő szakértőnek észrevételezés céljából. A szakterület vezetője, illetve a közreműködő szakértő a tervezet adatvédelmi folyamat tekintetében tett megállapításaira észrevételt tehetnek a tervezet megküldését követő 5 munkanapon belül. Az adatvédelmi jogi szakmai megállapítások tekintetében észrevétel nem tehető. Amennyiben az észrevétel megtételére nyitva álló határidő észrevétel megtétele nélkül eltelik, azt úgy kell tekinteni, hogy nincs észrevétel a tervezet tekintetében. Az észrevétel megtételére nyitva álló határidőre és a határidő elmulasztásának következményére az adatvédelmi tisztviselő a tervezet elküldése során felhívja a figyelmet. Az auditálással érintett szakterület részéről beérkezett észrevételeket az adatvédelmi tisztviselő 5 munkanapon belül értékeli, szükség esetén egyezteti a szakterülettel.

A tervezetek egyeztetését követően kialakított összefoglaló jelentést és az intézkedési tervet jóváhagyás céljából meg kell küldeni a vizsgálatot elrendelő személy és – amennyiben a vizsgálatot nem a vezérigazgató rendelte el – tájékoztatásként a vezérigazgató, valamint a Megfelelés támogatás szakterület vezetője részére. A 4.7.2.3. pont szerint lefolytatott adatvédelmi megfelelőségi vizsgálat keretében készült összefoglaló jelentést és intézkedési tervet a Társaság vezérigazgatója részére kell jóváhagyás céljából előterjeszteni. A vizsgálatot elrendelő személy az intézkedési terv kézhezvételét követő 5 munkanapon belül dönt annak jóváhagyásáról vagy részben / egészben történő elutasításáról. Az intézkedési terv jóváhagyása esetén annak végrehajtásáért az intézkedési tervben kijelölt szervezeti egység vezetője felelős. Amennyiben a vizsgálatot elrendelő személy részben vagy egészben nem hagyja jóvá intézkedési tervben foglalt javaslatokat, úgy írásban köteles megindokolni a javaslat figyelmen kívül hagyását, és ismertetnie kell azt, hogy a szervezeti egység által végzett adatkezelési tevékenység adatvédelmi megfelelőségét milyen módon biztosítja. E döntését az adatvédelmi tisztviselővel közli, amelyről – amennyiben a döntést nem a Társaság vezérigazgatója hozta meg – tájékoztatni kell a Társaság vezérigazgatóját és a Megfelelés támogatás szakterület vezetőjét. Amennyiben az elutasító döntésben ismertetett folyamat az adatvédelmi tisztviselő megítélése szerint továbbra sem felel meg az adatvédelmi követelményeknek, úgy erről tájékoztatja a vezérigazgatót és a Megfelelés támogatás szervezet vezetőjét. Amennyiben az intézkedési tervben foglalt javaslatok részben vagy egészben való elutasítására vonatkozó döntést nem a vezérigazgató hozta meg, úgy a döntést a vezérigazgató – az adatvédelmi tisztviselő által tett előterjesztésben foglaltak alapján – megváltoztathatja és az intézkedési tervet jóváhagyhatja, amelyről a vizsgálatot elrendelő személyt tájékoztatni kell.

Az intézkedési tervben szereplő javaslatok végrehajtására – figyelembe véve az intézkedés jellegét és az adatkezelési folyamat egyéb körülményeit – ésszerű időt szükséges biztosítani. Az intézkedési tervben megjelölt végrehajtási határidő legfeljebb egy alkalommal meghosszabbítható a végrehajtásra köteles szervezeti egység vezetőjének – adatvédelmi tisztviselő részére előterjesztett – indokolt kérelme alapján. Az adatvédelmi tisztviselő a végrehajtási határidő meghosszabbítására irányuló kérelmet – a végrehajtási határidő meghosszabbítására vonatkozó javaslatával együtt – továbbítja az intézkedési tervet jóváhagyó vezető részére. A kérelemben foglaltakról a kérelem előterjesztését követően döntést kell hozni. A kérelemről hozott döntésről az adatvédelmi tisztviselő tájékoztatja az intézkedési terv végrehajtására köteles szervezeti egység vezetőjét.

Az intézkedési terv végrehajtásában az adatvédelmi tisztviselő szakmai tanácsadásnyújtással közreműködik.

Az adatkezelő szervezeti egység vezetője az intézkedési terv végrehajtásáról a végrehajtására kijelölt határidőt követő 15 napon belül nyilatkozatot tesz az adatvédelmi tisztviselő részére.

4.7.5. Az adatvédelmi jelentésben foglaltak végrehajtásának ellenőrzése

Az adatvédelmi tisztviselő az intézkedési terv végrehajtását a végrehajtást követő hat hónap után ellenőrzi (a továbbiakban: monitoring vizsgálat). Az adatvédelmi tisztviselő a monitoring vizsgálat elvégzéséről és annak eredményéről feljegyzést készít. A monitoring vizsgálatot 30 napon belül el kell végezni. A monitoring vizsgálatról készült feljegyzést meg kell küldeni a vizsgálattal érintett szakterület vezetője részére. Amennyiben a monitoring vizsgálat során megállapításra kerül az adatkezelési folyamat adatvédelmi szabályoknak való nem megfelelősége, úgy az adatvédelmi tisztviselő az adatkezelő szervezeti egység részére javaslatot tesz a nem megfelelőség kiküszöbölésére vagy – amennyiben a nem megfelelőség súlya, jellege és körülményei indokolják – a vezérigazgató részére újabb audit lefolytatására.

Amennyiben a monitoring vizsgálat során megállapításra kerül, hogy az intézkedési terv megfelelően végrehajtásra került, úgy az adatvédelmi megfelelőségi vizsgálat – ideértve a vizsgálat iratanyagát is – lezárható.

4.7.6. Az adatvédelmi megfelelőségi vizsgálatok nyilvántartása

Az adatvédelmi megfelelőségi vizsgálatokról az adatvédelmi tisztviselő elektronikus nyilvántartást (a továbbiakban jelen alpont keretében: nyilvántartás) vezet. A nyilvántartást a Megfelelés támogatás szervezet részére a Társaság közös meghajtóján létrehozott szervezeti mappában a nyilvántartás vezetése céljából létrehozott önálló mappában kell vezetni, amelyhez az adatvédelmi tisztviselő, a Megfelelés támogatás vezető és az adatvédelmi szakértő rendelkezhet hozzáféréssel.

A nyilvántartás tárgyévi bontásban tartalmazza

a) a vizsgálat iktatószámát,
b) a vizsgálat tárgyát (a vizsgálattal érintett adatkezelési folyamatot),
c) a vizsgálattal érintett szervezeti egységet,
d) a vizsgálatot elrendelő személy beosztását vagy annak tényét, hogy a vizsgálat lefolytatására az éves auditálási terv alapján történt,
e) a vizsgálat kezdetének és befejezésének napját,
f) a vizsgálat során feltárt nem megfelelőségek és azok kiküszöbölésére tett intézkedési javaslatok rövid összegzését,
g) az összefoglaló jelentés és intézkedési terv jóváhagyásra történő előterjesztésének napját,
h) az összefoglaló jelentés és intézkedési terv jóváhagyásának vagy elutasításának napját,
i) az intézkedési terv végrehajtására kijelölt határidőt,
j) az intézkedési terv végrehajtásának napját,
k) a 4.7.5. pont szerint elvégzett monitoring vizsgálat időpontját és annak megállapításait.

A nyilvántartás tartalmát a Társaság vezérigazgatója, a Megfelelés támogatás vezető, az adatvédelmi tisztviselő, valamint a megfelelősségi vizsgálattal érintett szervezeti egység vezetője – kizárólag a szervezet által végzett adatkezelési folyamat tekintetében – ismerheti meg.

4.8. Az adatkezelési folyamat lezárásával kapcsolatos feladatok

Az adatkezelő szervezeti egység az adatkezelési folyamat befejezéséről egy példányban feljegyzést készít, amelyet az adatkezelési folyamattal összefüggő dokumentumokkal együtt – papír alapon és elektronikus úton egyaránt – megőriz. Az adatkezelő szervezeti egység a megszüntetett adatkezelési folyamat keretében kezelt személyes adatok törléséről, illetve a személyes adatokat tartalmazó adathordozók megsemmisítéséről – az egyedi adatkezelési folyamat tekintetében irányadó utasítás eltérő rendelkezése hiányában – a 16. számú függelék szerinti jegyzőkönyvet köteles felvenni. A feljegyzést és a jegyzőkönyvet az adatvédelmi tisztviselőnek – elektronikus úton – meg kell küldeni. Az adatkezelési folyamat megszüntetésének tényét és napját az adatkezelési nyilvántartásban rögzíteni kell és az erre vonatkozó adatokat 5 évig meg kell őrizni.

4.9. Mesterséges intelligencia alkalmazására vonatkozó rendelkezések

A mesterséges intelligencia alkalmazása során törekedni kell arra, hogy személyes adatok kezelésére ne kerüljön sor. A mesterséges intelligencia alkalmazásának valamely adatkezelési folyamatban történő bevezetésével összefüggésben elvégzett tesztelés kizárólag nem valós személyes adatokkal történhet. Amennyiben valamely adatkezelési folyamat keretében mesterséges intelligencia használatára kerül sor, úgy az előzetes hatásvizsgálat elvégzése kötelező.

5.0 HIVATKOZÁSOK, MÓDOSÍTÁSOK HATÁLYON KÍVÜL HELYEZÉSEK

5.1 Hivatkozások

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

- az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (GDPR),
- Magyarország Alaptörvénye,
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.),
- az Európai Adatvédelmi Testület (korábban: WP29-es munkacsoport), és a Nemzeti Adatvédelmi és Információszabadság Hatóság által elfogadott vélemények, ajánlások, tájékoztatók és közlemények,
- a munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.),
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.),
- a mindenkor hatályos Szervezeti és Működési Szabályzat,
- a mindenkor hatályos Informatikai Biztonsági Szabályzat,
- a mindenkor hatályos Iratkezelési Szabályzat,
- a mindenkor hatályos Kollektív Szerződés.

5.2 Hatályon kívül helyezések

Jelen utasítás hatályba lépésével egyidejűleg hatályát veszti az Adatvédelmi Szabályzatról szóló 39/2022. (VIII. 08.) számú vezérigazgatói utasítás, a VOLÁNBUSZ Zrt.adatvédelmi szabályzatáról szóló 95/EVU/2020. számú Elnök-vezérigazgatói Utasítás és a MÁV-HÉV Zrt. Adatvédelmi és Adatbiztonsági Utasításáról szóló, 30/2020. (VI.16.) számú vezérigazgatói utasítás.

5.3 MÁV Szolgáltató Központ Zrt. tájékoztatása

A normatív utasítást a MÁV Szolgáltató Központ Zrt. részére nem kell megküldeni.

5.4 Rendelkezések

Az utasítás függelékei az utasítás újbóli kiadása nélkül is aktualizálhatók, kiegészíthetők az utasítás karbantartásért felelős szervezet által. Az utasítás mindenkor hatályos függelékei a Társaság intranetes Utasítástárában érhetők el.

A jelen utasítás hatálybalépését követő egy éven belül a folyamatban lévő adatkezelési folyamatokat és az adatkezelési folyamatok tekintetében kiadott utasítások jelen utasításnak való megfelelését az adatkezelő szervezeti egység köteles felülvizsgálni.

A jelen utasítás kiadásáért felelős a jelen utasítást kétévente kötelezően felülvizsgálja, amelynek célja az utasítás rendelkezéseinek adatvédelmi jogszabályokkal való összhangjának biztosítása. A felülvizsgálat eredményét az adatvédelmi tisztviselő dokumentálja és az iratkezelési szabályoknak megfelelően megőrzi. A Társaság adatvédelmi rendszerét – ideértve az adatkezeléssel összefüggő feladatok megoszlását, hatásköröket és felelősségi szabályokat – érintő szervezeti változások esetén a jelen utasítást felül kell vizsgálni.

6.0 HATÁLYBA LÉPTETÉS

Jelen utasítás 2025. január 1. napján lép hatályba.

7.0 FÜGGELÉKEK

1. számú függelék: Adatkezelési tájékoztató (minta)
2. számú függelék: Adatvédelmi megfelelőségi vizsgálat megbízólevele
3. számú függelék: Belső adatvédelmi nyilvántartásba bejelentő lap
4. számú függelék: Az adatkezelésben részt vevő személyek minősítésének szempontrendszere
5. számú függelék: Adatvédelmi kockázatelemzés (minta)
6. számú függelék: Adatvédelmi hatásvizsgálat (minta)
7. számú függelék: Érdekmérlegelési teszt (minta)
8. számú függelék: Érintetti jogok gyakorlására vonatkozó áttekintés
9. számú függelék: Az érintett szóbeli kérelméről készített feljegyzés minta
10. számú függelék: Jegyzőkönyv személyes adatokba történő betekintési jog gyakorlásáról és annak biztosításáról
11. számú függelék: Adatvédelmi incidens bejelentő nyomtatvány
12. számú függelék: Összefoglaló jelentés adatvédelmi incidens vizsgálatáról (minta)
13. számú függelék: Adatvédelmi incidens nyilvántartás
14. számú függelék: Adatvédelmi incidens értékelési szempontjai
15. számú függelék: Folyamatábra az adatvédelmi incidens kezelésének folyamatáról
16. számú függelék: Adatmegsemmisítési jegyzőkönyv (minta)
17. számú függelék: Egyedi adattovábbítások nyilvántartása