ÉRTESÍTŐ

2022/31. SZÁM

TARTALOM

Utasítások **oldal**

31. szám Budapest, 2022. május 04.

30/2022. (V. 04. MÁV-START Ért. 31.) sz. vezérigazgatói utasítás az Adatvédelmi Szabályzatról

1.0 AZ UTASÍTÁS CÉLJA

Az utasítás célja, hogy a vonatkozó adatvédelmi jogszabályok tükrében meghatározza a MÁV-START 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 szabályokat, minimumkövetelményeket. 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 és adatfeldolgozásra, amely személyes adatra vonatkozik, függetlenül attól, hogy az adatkezelés, illetve adatfeldolgozás 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.

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

Az utasítás elkészítéséért és szükség szerinti módosításáért a Társaság Megfelelés Támogatás vezetője és az Adatvédelmi tisztviselő 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 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 – munkavállalókból 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 adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.

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) 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 Nemzeti Adatvédelmi és Információszabadság Hatóság állásfoglalásai, iránymutatásai, ajánlásai és döntései.

Adatvédelmi szakértők: az adatvédelmi tisztviselő közvetlen irányítása alatt álló szakértő(k), akik segítik az adatvédelmi tisztviselő munkáját.

Adattovábbítás: az adat meghatározott harmadik fél számára történő hozzáférhetővé tétele.

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.

Automatizált döntéshozatal: amikor a személyes adatok kezelése során folytatott eljárás 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. ujjlenyomat).

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 az 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.

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.

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 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, vagy 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 Társaság munkavállalói munkajogi, polgári jogi és büntető jogi 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 Vezérigazgató

a) Meghatározza, illetve jóváhagyja a Társaság adatkezeléssel járó tevékenységeinek adatvédelmi követelményeit.
b) Jelen utasítás keretei között:
   - Meghatározza az adatvédelem szervezeti rendszerét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket.
   - Biztosítja a Társaság által végzett adatkezelések jogszerűségének feltételeit.
   - 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 módosításáról.
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 nagy számú 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 hivatalból vagy megbízólevél alapján lefolytatja az adatvédelmi megfelelőségi vizsgálatot, amely során ellenőrzi az egyes adatkezelési folyamatok adatvédelmi jogszabályoknak való megfelelését.
d) Minden tárgyév *január 31*. napjáig jóváhagyásra előterjeszti a Vezérigazgató részére az éves 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) A Társaság nevében kapcsolatot tart és együttműködik az adatvédelmi felügyeleti hatósággal.
j) Vezeti a Társasági szintű adatkezelési tevékenységek nyilvántartását és a részére bejelentett adatvédelmi incidenseket tartalmazó nyilvántartást.
k) Minden tárgyév január 31. napjáig írásban éves jelentést készít a tárgyévet megelőző év Társaságot érintő legfontosabb adatvédelmi kérdéseiről, amelyet megküld a Vezérigazgató részére.
l) 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 GPDR 38. cikkét kell alkalmazni azzal, hogy feladatait a Megfelelés támogatás szervezet keretében látja el.

4.2.5 Biztonsági Igazgatóság Informatikai biztonsági és titokvédelmi 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, informatikai biztonsági és titokvédelmi érintettségű adatvédelmi incidensek kivizsgálásában.

4.2.6 Marketing és utastájékoztatás 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 – jelöli 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 kockázatelemzésben, 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 stb. 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, az ülésen történt események leírását, az ülésen elhangzott nyilatkozatok – szükség esetén szó szerinti – leiratát, valamint más, az ülés dokumentálása szempontjából lényeges információt.

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 igazolására szolgáló intézkedéseket az egyes adatkezelési folyamatokat szabályozó belső utasításaiban szükséges meghatározni.

4.4 A személyes adatok kezelésének jogalapjai

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.

4.4.1 A személyes adatok kezelésének jogalapjai

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 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 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 kezelése

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 vagy;

- 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.

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 – 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 – 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.

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 arról, hogy kik és milyen célból kapják vagy kapták meg az érintett személyes adatait, illetve az érintettet az adatkezeléssel összefüggő jogairól.

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

bb) Másolat kéréshez 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 titkosított 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 kért másolat ingyenes, azonban minden további másolatért észszerű mértékig a Társaság költségtérítést állapíthat meg.

A másolat kéréshez való jog teljesítése nem érintheti hátrányosan mások jogait és szabadságait.

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 betekintsen.

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 írásban 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 az adatkezelés célja megszűnt, ha az érintett visszavonja hozzájárulását, ha azok kezelése jogellenes, ha az adatok tárolásának meghatározott határideje lejárt, továbbá ha azt bíróság vagy hatóság elrendelte, valamint ha 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:

- 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.
- Jogellenes adatkezelés: a nem a GDPR-ban foglaltaknak, illetve a vonatkozó előírásoknak megfelelő adatkezelés esetén az érintett jogosult a személyes adatok törlését kérni, a Társaság – a jogellenes adatkezelés megállapítása esetén – köteles azok törlésére.
- Az adatkezelés célja megszűnt vagy teljesült, de az érintettnek szüksége van a személyes adatokra jogi igények előterjesztéséhez, érvényesítéséhez, védelméhez.
- 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 aránytalan nagy erőfeszítést igényel. Az érintettet kérésére a Társaság tájékoztatja e 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.

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.

4.5.2 Az érintetti jogok gyakorlására vonatkozó szabályok

Érintetti jog gyakorlására irányuló kérelmet 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.

4.5.2.1 Az érintetti jogok gyakorlásának módja

Az érintett a jogainak gyakorlására irányuló 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 8. számú melléklet 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 8. számú melléklet 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.

4.5.2.2 Az érintetti jog gyakorlására irányuló kérelem teljesítése

A kérelem beérkezését követően az adatgazda szervezeti egység haladéktalanul 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.

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 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. 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 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 kell igazolnia.

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 GPDR 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 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 végezi 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 Igazgatóság Informatikai biztonsági és titokvédelmi 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, ideértve az adatkezelés technikai megvalósítását, valamint az adatkezelés tervezett időtartamát és az adatkezelés jogalapját. 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. Az adatkezelés kockázatát a „valószínűség” és „hatás” „mátrix-rendszerében” kell meghatározni az 1. számú mellékletben foglalt szempontok szerint. A kockázatelemzés során az 1. számú mellékletben meghatározott értékelési szempontok mérlegelésére van szükség. Az adatvédelmi tisztviselő szükség esetén állásfoglalást bocsáthat ki a további értékelési szempontok meghatározására.

A kockázatelemzés keretében megállapított kockázati szint 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.

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 15 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 1. számú melléklet 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 Átmeneti rendelkezések

A jelen utasítás hatálybalépésekor folyamatban lévő adatkezelési folyamatok kockázatelemzését a hatályba lépést követő harmadik 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.

4.6.2 Adatvédelmi hatásvizsgálat

Amennyiben az Adatkezelő szervezeti egység a személyes adatok kezelésével járó tevékenység tervezésekor úgy ítéli meg, hogy az az érintettek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal jár, akkor a tervezési folyamat részeként 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 a 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) pontban foglalt jogalap biztosítja és a vonatkozó jogszabály szabályozza az adott adatkezelési műveletet, valamint ezen 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 2. számú melléklete 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 adatkezelés jogalapjának meghatározása

Az adatkezelő szervezeti egység az adatkezelési folyamat tervezése során, legkésőbb az adatkezelés megkezdését megelőzően 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 szüksége-e. Amennyibben 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 3. számú mellékletben 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) bekezdésben meghatározott valamely feltétel fennállását igazolni kell, ennek hiányában a személyes adatok különleges kategóriájába tartozó személyes adat kezelése tilos.

4.6.3.2 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 5. számú mellékletben foglalt minta alapján – az adatvédelmi tisztviselő közreműködésével – elkészíti az adatkezelési tájékoztatót. Az 5. számú melléklet szerinti adatkezelési tájékoztató minta szövegétől az adatkezelési folyamat jellegére és az adatkezelés körülményeire tekintettel el lehet térni.

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.

Az adatkezelési tájékoztató közlésére vonatkozó szabályok:

Az adatkezelési tájékoztató közlésének kötelezettségére vonatkozó szabályokat – 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 tételre van szükség. Amennyiben az adatkezelés jogszerűségét az érintett hozzájárulása biztosítja, az adatkezelési tájékoztatót a hozzájáruló nyilatkozat megtételét megelőzően meg kell ismertetni. Az adatkezelési tájékoztató megismeréséről az érintettet minden esetben 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-ban 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 az adatkezelési tájékoztatót tartalmazó utasításnak közzétételével vagy az adatkezelési tájékoztató munkáltatói jogkör gyakorló részére elektronikus úton történő megküldésével közli, mindezt azzal, hogy a munkáltatói jogkörgyakorlója köteles valamennyi, az irányítása alatt lévő érintett részére elektronikus úton vagy a helyben szokásos módon (pl. parancskönyvi rendelkezés kiadásával) megküldeni az adatkezelési tájékoztatót.

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 elektronikus elérhetőséggel rendelkező érintettek részére a „Közös meghajtón”,
b) az elektronikus elérhetőséggel nem rendelkező érintettek részére a helyben szokásos módon
c) kell közzé tenni és biztosítani annak elérhetőségét.

Helyben szokásos módon történő közzététel teljesíthető azzal, hogy a munkavállaló érintett 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.

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.

4.6.3.3 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 adatvédelmi tisztviselő mellett a Biztonsági Igazgatóság Informatikai biztonsági és titokvédelmi szakterületének bevonása is szükséges. Az adatbiztonsági intézkedések meghatározása során az IBSZ rendelkezéseit figyelembe kell venni.

4.6.4 Az adatkezelési tevékenységek nyilvántartása

Az Adatkezelő szervezeti egységek az általuk végzett adatkezelési folyamatokról kötelesek nyilvántartást vezetni. Az Adatkezelő szervezeti egység az általa vezetett nyilvántartást elektronikus úton megküldi az Adatvédelmi tisztviselő részére a Társasági szintű adatvédelmi tevékenységek nyilvántartása céljából. Az adatkezelési tevékenységek nyilvántartásában szereplő bármely adatkezelési folyamat változása, illetve új adatkezelési folyamat felvétele esetén az adatkezelő szervezeti egység a 4. számú melléklet szerinti formanyomtatvány alkalmazásával haladéktalanul köteles adatot szolgáltatni az adatvédelmi tisztviselő részére.

Az adatvédelmi tisztviselő szakmai iránymutatást ad az adatkezelő szervezeti egységek részére az adatkezelési tevékenységek nyilvántartásának vezetéséhez.

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,
   bc) az adatkezelés jogalapját,
   bd) az érintettek kategóriáit,
   be) a kezelt személyes adatok kategóriáit,
   bf) a személyes adatok forrása,
   bg) az adatkezelési folyamatra irányadó jogszabály vagy belső szabályozó megjelölése,
   bh) a személyes adatok megőrzésének időtartama vagy az adatkezelés időtartamának meghatározásának szempontjai,
   bi) az adatkezelési folyamatra vonatkozó adatkezelési tájékoztató megléte, illetve annak elérhetősége,
   bj) a személyes adatok továbbítására vonatkozó információ azzal, hogy amennyiben a személyes adatok valamely címzett(ek) részére továbbításra kerülnek, úgy legalább a címzett(ek) kategóriájának megjelölése.
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.

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 vagy adatfeldolgozójának munkavállalója észleli, hogy a Társaságnál olyan esemény történt, amely feltehetően adatvédelmi incidensnek minősül, úgy haladéktalanul, de legkésőbb 4 órán belül köteles elektronikus úton írásban (e-mail), valamint telefonon értesíteni az adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő az értesítést követően haladéktalanul felveszi a kapcsolatot az adatvédelmi incidenssel érintett adatkezelő szervezeti egység (egységek) vezetőjével. Amennyiben az adatvédelmi incidens elektronikus úton végzett adatkezelési folyamatot érint, úgy értesíteni kell a Biztonsági Igazgatóság Informatikai biztonsági és titokvédelmi 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.

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 ki kell vizsgálni. 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 tájékoztatja a Társaság Vezérigazgatóját.

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

Az adatvédelmi incidens kivizsgálása:

Adatvédelmi incidens kivizsgálására az adatvédelmi tisztviselő vizsgáló bizottságot alakít. A vizsgálóbizottságot úgy kell kialakítani, hogy az adatvédelmi incidens kivizsgálása akadálymentesen megvalósuljon. A vizsgáló bizottság tagja:

a) az adatvédelmi tisztviselő,
b) az adatvédelmi incidenssel érintett adatkezelő szervezeti egység vezetője (vezetői),
c) amennyiben az adatvédelmi incidens elektronikus úton végzett adatkezelést érint, úgy a Biztonsági Igazgatóság információvédelmi szakértője,
d) amennyiben az adatvédelmi incidens informatikai rendszert érint, az Informatika szervezet vezetője, vagy az általa kijelölt személy,
e) amennyiben az adatvédelmi incidens a Társaság munkavállalóinak személyes adatait érinti, úgy a Humánerőforrás Igazgató által kijelölt munkavállaló,
f) az adatvédelmi incidens jellegétől függően szükség szerint más szakterület vezetője által 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, az adatvédelmi incidensben érintett személyes adatok jellegét és számát, az adatvédelmi incidens ismert következményeit.

Az adatvédelmi incidenseket jellegük 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 kockázatait. A kockázatelemzés célja, hogy a Társaság értékelje azt, hogy az adatvédelmi incidens milyen hatással van az érintettek jogaira és szabadságaira.

Az adatvédelmi incidens kockázatelemzése 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.

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, jellege,
- a személyes adatok típusa (pl. különleges adat) és mennyisége,
- lehetséges-e az érintettek azonosítása, ha igen, az könnyen megvalósulhat-e,
- milyen súlyú következményei vannak az incidensnek az érintettre nézve,
- az adatvédelmi incidensben érintett személyek speciális kategóriái,
- az érintettek száma,
- 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, az incidensben 16. életévet be nem töltött személyek is érintettek, az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre.

Az adatvédelmi incidenssel kapcsolatos intézkedési terv

A vizsgáló bizottság az adatvédelmi incidens kivizsgálása során feltárt információk alapján 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 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

Az adatvédelmi incidenst az adatvédelmi tisztviselő indokolatlan késedelem nélkül, de legkésőbb az adatvédelmi incidens tudomására 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 érintett személyes adatok kategóriái és – legalább hozzávetőleges – száma,
- az adatvédelmi tisztviselő neve, elérhetősége,
- az adatvédelmi incidensből eredő, valószínűsíthető következmények.

Az érintettek tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő szervezeti egység 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 értelmezhetőek.
- 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 tisztviselő az adatvédelmi incidens következményeként szükség esetén állásfoglalást ad ki arról, hogy az adatkezelő szervezeti egységeknek milyen további intézkedések megtételét javasolja az adatvédelmi incidensek 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 6. számú melléklet szerinti tartalommal nyilvántartja az adatvédelmi incidenseket.

4.6.6 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.

4.7 Adatvédelmi megfelelőség ellenőrzése

4.7.1 Az adatvédelmi 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 vizsgálat elrendelése

A vizsgálat 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 7. számú melléklet szerinti megbízólevél megfelelő kitöltésével és az adatvédelmi tisztviselő részére történő megküldésével rendelheti el. A b) – c) pontban megjelölt, a vizsgálat elrendelésére jogosult személy a megbízólevél kibocsátását megelőzően köteles a vizsgálat elrendelésére vonatkozó szándékát jóváhagyatni a Társaság Vezérigazgatójával. Az audit elrendelését követően, a vizsgálat elrendeléséről – a vizsgálat elvégzésére vonatkozó megbízólevél megküldésével együtt – a Társaság Vezérigazgatóját haladéktalanul, de legkésőbb a megbízólevél kézhezvételét követő két munkanapon belül tájékoztatja az adatvédelmi tisztviselő.

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.

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 30 napot szükséges biztosítani, amely nem lehet több 60 napnál. Az adatvédelmi tisztviselő negyedévente – ide nem értve az éves auditálási terv szerint lefolytatott vizsgálatot – összesen legfeljebb három vizsgálat lefolytatásával bízható meg.

Az adatvédelmi tisztviselő minden tárgyév *január 31. napjáig* elkészíti és a Vezérigazgató részére jóváhagyás céljából megküldi a 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.

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 vizsgálatok tekintetében a jelen fejezet szabályait megfelelően alkalmazni kell.

Az auditálási terv Vezérigazgató által történt jóváhagyása esetén nincs szükség a 7. számú melléklet szerinti megbízólevél kibocsátására. Az első auditálási tervet a jelen utasítás hatálybalépését követő 30 napon belül kell jóváhagyásra megküldeni a Vezérigazgató részére. Az első auditálási tervben a jelen utasítás hatálybalépését követő negyedévek tekintetében kell meghatározni a vizsgálni kívánt adatkezelési folyamatokat.

4.7.3 Az adatvédelmi 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 dokumentumba 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 határidő meghosszabbítására irányuló kérelmet az adatvédelmi tisztviselő a vizsgálatot elrendelő személy részére terjeszti elő, amelyben meg kell jelölni a határidő meghosszabbítását indokoló körülményeket. A határidő meghosszabbítására irányuló kérelemről három napon belül döntést kell hozni.

4.7.4 Az adatvédelmi vizsgálat befejezése

Az adatvédelmi tisztviselő a vizsgálat elvégzését követő 15 napon belül összefoglaló jelentést (a továbbiakban: összefoglaló jelentés) készít, amely tartalmazza a vizsgált adatkezelési folyamat adatvédelmi megfelelősége tekintetében tett megállapításokat, illetve a nem megfelelőség megállapítása esetén annak kiküszöbölésére alkalmas megoldási javaslatot, illetve javaslatokat, továbbá a nem megfelelőség kockázatait, lehetséges jogkövetkezményeit.

Az összefoglaló jelentést 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. Az összefoglaló jelentésben szereplő javaslatok végrehajtására – figyelembe véve az intézkedés jellegét és az adatkezelési folyamat egyéb körülményeit – ésszerű időt szükséges biztosítani.

A vizsgálatot elrendelő személy az összefoglaló jelentés kézhezvételét követő 5 munkanapon belül dönt az adatvédelmi tisztviselő által az összefoglaló jelentésben foglalt javaslatok jóváhagyásáról vagy azok részben vagy egészben történő elutasításáról. Az összefoglaló jelentés és az abban foglalt javaslatok jóváhagyása esetén az abban foglaltak végrehajtásáért az Adatkezelő szervezeti egység felelős. Az összefoglaló jelentés végrehajtásában az adatvédelmi tisztviselő szakmai tanácsadás-nyújtással közreműködik.

Amennyiben a vizsgálatot elrendelő személy részben vagy egészben nem hagyja jóvá az összefoglaló jelentésben 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 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 összefoglaló jelentésben foglalt javaslatok részben vagy egészben való elutasításra vonatkozó döntést nem a Vezérigazgató hozta meg, úgy a döntést a Vezérigazgató saját hatáskörben megváltoztathatja, és az összefoglaló jelentést jóváhagyhatja, amelyről a vizsgálatot elrendelő személyt tájékoztatni kell.

Az adatkezelő szervezeti egység vezetője az összefoglaló jelentésben megjelölt és jóváhagyott javaslatok végrehajtásáról a javaslatok végrehajtására kijelölt határidőt követő 30 napon belül nyilatkozatot tesz.

4.7.5 Az adatvédelmi jelentésben foglaltak végrehajtásának ellenőrzése

Az adatvédelmi tisztviselő az összefoglaló jelentésben foglalt javaslatok megfelelő végrehajtását a végrehajtásra kijelölt határidőt követő hat hónapot követően ellenőrzi (a továbbiakban: monitoring

vizsgálat). Az adatvédelmi tisztviselő a monitoring vizsgálat elvégzéséről és annak eredményéről feljegyzést készít. A monitoring vizsgálatot 15 napon belül el kell végezni. A monitoring vizsgálatról készült feljegyzést meg kell küldeni a Vezérigazgató, az Adatkezelő szervezeti egység és a Megfelelés támogatás 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.

4.7.6 Az adatvédelmi tisztviselő által saját hatáskörben lefolytatott adatvédelmi vizsgálat

Az adatvédelmi tisztviselő saját hatáskörben, a 4.7.2. pont szerinti elrendelés nélkül is végezhet adatvédelmi megfelelőségi vizsgálatot valamely adatkezelési folyamat adatvédelmi megfelelőségének biztosítása érdekében. A lefolytatott vizsgálat tekintetében a jelen fejezet szabályait kell alkalmazni azzal az eltéréssel, hogy a vizsgálat eredményéről és a feltárt hiányosságok kiküszöbölése érdekében tett javaslatokról az Adatkezelő szervezeti egység vezetőjét a vizsgálat lefolytatását követő 15 napon belül kell tájékoztatni.

4.7.7 Az adatvédelmi megfelelőségi vizsgálatok nyilvántartása

Az elrendelt és lefolytatott adatvédelmi vizsgálatokról az adatvédelmi tisztviselő elektronikus nyilvántartást vezet.

A nyilvántartás tárgyévi bontásban tartalmazza a lefolytatott vizsgálat iktatószámát és tárgyát, a vizsgálattal érintett szervezeti egységet, a vizsgálatot elrendelő személy beosztását, a vizsgálat kezdetének napját, az összefoglaló jelentés jóváhagyásra történt előterjesztésének napját, valamint az összefoglaló jelentés jóváhagyásának vagy elutasításának napját. A nyilvántartásban röviden ismertetni kell a vizsgálat során feltárt hiányosságokat és az azok kiküszöbölésére tett és jóváhagyott javaslatot, továbbá a javaslat végrehajtására kijelölt határidőt, valamint a javaslat végrehajtásáról szóló nyilatkozat megtételének napját. A nyilvántartásba be kell jegyezni a 4.7.5. pont szerint elvégzett monitoring vizsgálatról készült feljegyzés megállapításait és a monitoring vizsgálat időpontját.

A nyilvántartás tartalmát a Társaság Vezérigazgatója, a Megfelelés támogatás vezető, az adatvédelmi tisztviselő, a megfelelősségi vizsgálattal érintett szervezeti egység vezetője 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 – 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.

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.

5.2 Módosítások
Nincsenek.

5.3 Hatályon kívül helyezések
Az utasítás hatályba lépésével egyidejűleg hatályát veszti az Adatvédelmi Szabályzatról szóló 45/2019. (VII. 18. MÁV-START Ért. 30.) sz. vezérigazgatói utasítás.

5.4 MÁV Szolgáltató Központ Zrt. tájékoztatása
A normatív utasítást tartalmazó MÁV-START Értesítőt a MÁV Szolgáltató Központ Zrt. részére *meg kell küldeni*/nem kell megküldeni.

5.5 Vezérigazgatói meghatalmazás
Jelen utasításhoz nem szükséges.

5.6 Rendelkezések
Jelen utasításhoz nincsenek.

6.0 HATÁLYBA LÉPTETÉS
Jelen szabályzat a MÁV-START Értesítőben történő közzétételt követő 15. napon lép hatályba és visszavonásig érvényes.

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.

7.0 MELLÉKLETEK
1. számú melléklet:
„Adatvédelmi kockázatelemzés” minta

2. számú melléklet:
„Adatvédelmi hatásvizsgálat” minta

3. számú melléklet:
„Érdekmérlegelési teszt” minta

4. számú melléklet:
„Belső adatvédelmi nyilvántartásba bejelentő lap” minta

5. számú melléklet:
„Adatkezelési tájékoztató” minta

6. számú melléklet:
„Adatvédelmi Incidens nyilvántartás” minta

7. számú melléklet:
„Adatvédelmi megfelelőségi vizsgálat megbízólevele”

8. számú melléklet:
„Az érintett szóbeli kérelméről készített feljegyzés” minta

9. számú melléklet:
„Folyamatábra az érintetti kérelem elbírálásának és teljesítésének folyamatáról”

10. számú melléklet:
„Folyamatábra az adatvédelmi incidens kezelésének folyamatáról”

Keresztes Péter s.k.
vezérigazgató

Iktatószám: …../……/START

ADATVÉDELMI KOCKÁZATELEMZÉS
(minta)

Adatkezelő megnevezése:	**MÁV-START Zrt.**
Adatkezelő szervezeti egység(ek) megnevezése:	
Az adatvédelmi kockázatelemzéssel érintett adatkezelési folyamat:	
A kockázatelemzés elvégzésének oka:	Új adatkezelési folyamat megkezdése / meglévő adatkezelési folyamat felülvizsgálata
Az adatvédelmi kockázatelemzés elvégzésének dátuma:	20… (év) …… (hó) ….. (nap)
Az adatvédelmi kockázatelemzéssel érintett adatkezelési folyamat megkezdésének tervezett ideje:	20… (év) …… (hó) ….. (nap)
A kockázatelemzést végző személy:	Név, beosztás
A kockázatelemzésbe bevont más szakterület képviselője:	Név, beosztás, szakterület
A kockázatelemzésbe bevont információvédelmi szakember:	Név, beosztás
A kockázatelemzésbe bevont adatvédelmi tisztviselő:	Név
A kockázatelemzés felülvizsgálatának időpontja(i):	I. 20… (év) …… (hó) ….. (nap) II. 20… (év) …… (hó) ….. (nap) III. 20… (év) …… (hó) ….. (nap)

ADATVÉDELMI KOCKÁZATELEMZÉS

AZ ADATKEZELÉSI FOLYAMAT PONTOS, RÉSZLETES LEÍRÁSA:

AZ ADATKEZELÉS JOGSZERŰ CÉLJÁNAK ÉS JOGALAPJÁNAK PONTOS, KONKRÉT LEÍRÁSA:

AZ ADATKEZELÉS SORÁN KEZELT SZEMÉLYES ADATOK ÉS ÉRINTETTEK KÖRE:

AZ ADATKEZELÉS KOCKÁZATÁNAK SZÖVEGES ÉRTÉKELÉSE:

AZ ADATKEZELÉS KOCKÁZATAINAK KEZELÉSE ÉRDEKÉBEN TETT INTÉZKEDÉSEK:

AZ ADATVÉDELMI KOCKÁZATELEMZÉST KÉSZÍTETTE:

……..
Név, beosztás, aláírás

AZ ADATVÉDELMI TISZTVISELŐ ÉRTÉKELÉSE:

……
Név, aláírás

AZ ADATVÉDELMI KOCKÁZATELEMZÉST JÓVÁHAGYTA:

……
Név, beosztás, aláírás

AZ ADATVÉDELMI KOCKÁZATELEMZÉS FELÜLVIZSGÁLATÁNAK MEGÁLLAPÍTÁSAI:

AZ ADATVÉDELMI KOCKÁZATELEMZÉS FELÜLVIZSGÁLATÁT ELVÉGEZTE ÉS JÓVÁHAGYTA:

……..
Név, beosztás, aláírás

……..
Név, beosztás, aláírás

Az adatvédelmi kockázatelemzés elvégzésének szempontrendszere

Valószínűség	*Nagyon magas*	Közepes	Magas	Nagyon magas	Nagyon magas
	Magas	Alacsony	Magas	Nagyon magas	Nagyon magas
	Alacsony	Alacsony	Közepes	Magas	Nagyon magas
	Valószínűtlen	Alacsony	Alacsony	Közepes	Nagyon magas
		Elhanyagolható	*Korlátozott*	*Jelentős*	*Nagyon jelentős*
		Hatás			

A kockázat hatása annak a vizsgálatát jelenti, hogy milyen rövid, közép és hosszú távú következménye lehet annak, hogy az adatkezelési folyamat során az adatkezelő nem alkalmaz az érintett jogainak és szabadságainak védelme érdekében megfelelő szintű adatbiztonsági (szervezési és technikai) intézkedéseket. A kockázat hatása annak függvényében változik, hogy annak bekövetkezése milyen következménnyel jár az érintett számára.
A kockázat hatását az alábbi kategóriákba sorolhatjuk: „nagyon jelentős”, „jelentős”, „korlátozott” és „Elhanyagolható”.
a) Nagyon jelentős a kockázat hatása, ha az
- az érintettet megillető alapvető jogokat és szabadságokat érint és annak következménye visszafordíthatatlan,
- ha az a személyes adatok különleges kategóriájába tartozó személyes adatot vagy a bűnügyi személyes adatot érint és annak következménye visszafordíthatatlan,
- az érintett részére visszafordíthatatlan vagyoni vagy nem vagyoni károkat okoz,
- visszafordíthatatlan következményeket okoz az érzékeny kategóriába tartozó érintett részére (pl. ha az érintett kiskorú gyermek, fogyatékkal élő személy, idős korú személy stb.),
- az érintett részére visszafordíthatatlan szociális károkat okoz, különösen, ha az diszkriminatív.

b) Jelentős a kockázat hatása, ha
- a kockázat nagyon jelentős kockázatnak minősül, de annak következménye visszafordítható,
- az érintett személyes adatok fölötti rendelkezési jogának teljes elvesztését eredményezi, különösen a személyes adatok vagy az érintettek magas számára tekintettel,
- az érintett személyes adatok fölötti rendelkezési jogának legfeljebb részleges elvesztését eredményezi, feltéve, ha a személyes adat különleges adatnak vagy bűnügyi személyes adatnak minősül,
- az érintett személyazonosságának lopása következik vagy következhet be,
- az érintettet jelentős pénzügyi veszteség érheti,
- a szakmai titoktartási kötelezettség alá eső személyes adatok bizalmassága sérül,
- az érintetteket vagy az érintettek bizonyos csoportját társadalmi sérelem éri.

c) Korlátozott a kockázat hatása, ha
- az érintett személyes adatok fölötti rendelkezési jogának legfeljebb részleges elvesztését eredményezi,
- elhanyagolható pénzügyi veszteséget eredményezhet az érintett részére.

d) Elhanyagolható a kockázat hatása, ha annak következményei maradéktalanul helyreállíthatóak.

A kockázatok bekövetkezésének valószínűségét az alábbi kategóriákba sorolhatjuk: „nagyon magas”, „magas”, „alacsony” és a „valószínűtlen” kockázat.
a) Nagyon magas a kockázat bekövetkezésének valószínűsége, ha
- ha az adatkezelés során olyan technológia alkalmazására kerül sor, amely a WP248 számú iránymutatás szerint magas kockázatúnak minősül függetlenül annak valószínűségétől,
- vannak olyan auditok/tanulmányok, amelyek azonosítják a kockázathoz kapcsolódó szervezeti eljárások vagy technikai eszközök lényeges sebezhetőségeit;

- rendelkezésre állnak olyan információk, amelyek igazolják azt, hogy a kockázat más adatkezelőknél az elmúlt egy év során bekövetkezett,
- az adatkezelést megelőző egy éven belül a Társaságnál a kockázat már bekövetkezett.

b) Magas a kockázat bekövetkezésének valószínűsége, ha
- az adott körülmény az elmúlt egy év során legalább egy alkalommal bekövetkezett a Társaságnál;
- vannak olyan auditok/tanulmányok, amelyek azonosítják a kockázathoz kapcsolódó szervezeti eljárások vagy technikai eszközök lehetséges sebezhetőségeit;
- a kockázati tényezőkhöz kapcsolódó elemeket nem kiforrott technológiákkal vagy szervezeti eljárásokkal, minőségi szabványok betartása nélkül, független harmadik felek általi tanúsítás nélkül hajtották végre.

c) Alacsony valószínűségűnek minősül a kockázat, ha az adott körülmény az elmúlt tíz év során egy alkalommal következett be a Társaságnál.
d) Valószínűtlennek minősül a kockázat, ha nincs semmilyen körülmény, amely az adott kockázat bekövetkezését igazolja.

Értékelési szempontok az adatkezelés kockázatának megállapításához (WP248*)

Az adatkezelési folyamat kockázatainak értékelése során az alábbi szempontokat szükséges mérlegelni:

a) Értékelés vagy pontozás, ideértve a profilalkotást és az előrejelzést is, különösen az érintett munkahelyi teljesítményére (pl. teljesítményalapú bérezés), gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján.
b) Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: adatkezelés, amelynek célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala (pl. elektronikus úton történő szerződéskötés természetes személy beavatkozása nélkül).
c) Módszeres megfigyelés: érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztüli adatgyűjtés vagy a nyilvános helyek nagymértékű, módszeres megfigyelése (pl. kamerás megfigyelőrendszer alkalmazása; GPS nyomkövető alkalmazása az érintettek megfigyelésére).
d) Különleges adatok vagy fokozottan személyes jellegű adatok kezelése (pl. különleges adatok esetén: egészségügyi adatok, illetve szakszervezeti tagságra vonatkozó adatok kezelése, valamint fokozottan személyes jellegű adatok kezelése az érintett személyiségének ellopására alkalmas személyazonosító adatok, illetve pénzügyi adatok).
e) Személyes adatok nagy számban történő kezelése, amelynek meghatározása során az alábbi tényezőket kell figyelembe venni:
- az érintettek száma konkrét számadatként vagy a lakosság arányában
- a kezelt adatok mennyisége vagy adatfajták köre
- az adatkezelési tevékenység időtartama vagy állandó jellege
- az adatkezelési tevékenység földrajzi kiterjedése.

* A 29. cikk alapján létrehozott Adatvédelmi Munkacsoport iránymutatása az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e (WP248). Elérhető: https://naih.hu/edpb-iranymutatasai

f) Adatkészletek egymással való megfeleltetése vagy összevonása például két vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett ésszerű elvárásait meghaladó módon (pl. két eltérő célból végzett adatkezelés adatbázisának interfészen keresztül történő összekapcsolása).

g) Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok. Kiszolgáltatott helyzetben lévő érintettnek kell tekinteni a gyermekeket, munkavállalókat, lakosság különleges védelmet igénylő rétegei (idősek, fogyatékossággal élők, betegségben szenvedő személyek) vagy minden olyan esetet, amikor az érintett és az adatkezelő közötti kapcsolatban egyenlőtlen helyzet (alá-fölé rendeltségi viszony) alakul ki.

h) Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: például az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében.

i) Azok az esetek, amikor az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek. Ide tartoznak az érintettek számára szolgáltatás igénybevételének vagy szerződéskötésnek a lehetővé tételére, módosítására vagy elutasítására irányuló adatkezelési műveletek.

Minél több az előzőekben felsorolt szempontnak felel meg az adatkezelés, annál nagyobb a valószínűsége annak, hogy az magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

ADATVÉDELMI HATÁSVIZSGÁLAT
(minta)

1. Az adatvédelmi hatásvizsgálattal érintett adatkezelési folyamat:
Adatkezelési folyamat megnevezése és szerepkörök meghatározása a hatásvizsgálatban (készítő, felülvizsgáló, jóváhagyó)

2. Adatkezelés leírása:
Az adatkezelés rövid bemutatása, különösen az adatkezelés célja, jogalapja, kezelt adatok köre és egyéb lényeges körülmények. *Az adatkezeléshez kapcsolódó felelősségi viszonyok bemutatása. Az adatkezelésben közreműködő felek, adatkezelő, adatfeldolgozó közös adatkezelő, ezek egymáshoz való viszonya, és felelősségi körök megoszlása.* *Rendelkezik-e az adatkezelésre alkalmazandó valamilyen szabvánnyal? Szabványok, magatartási kódexek, tanúsítványok felsorolása, amennyiben vannak ilyenek.*

3. Adatok, adatkezelés folyamata:
A kezelt személyes adatok köre. Sorolja fel a gyűjtött és kezelt adatokat. Egyenként (vagy kategóriánként) határozza meg a tárolás időtartamát, az esetleges címzetteket és azokat a személyeket, akik az adatokhoz hozzáférnek. *Az adatkezelési folyamatok bemutatása. Mutassa be az adatkezelés folyamatát (az adatgyűjtéstől az adatok megsemmisítéséig, az adatkezelés különböző szakaszait, a tárolást stb.), használjon például a személyes adatok útját - adatfolyamot - bemutató ábrát (melyet mellékletként feltölthet).* *Melyek a személyes adatok kezelésére szolgáló eszközök? Sorolja fel a személyes adatok kezelésére szolgáló eszközöket (operációs rendszerek, alkalmazások, adatbázis-kezelő rendszerek, helyiségek, egyéb eszközök stb.)*

4. Adatkezelés célja, jogalapja, tárolás időtartama:
Az adatkezelés céljai meghatározottak-e, egyértelműek-e és jogszerűek-e? Fejtse ki, hogy mitől meghatározottak, egyértelműek és jogszerűek az adatkezelés céljai. *Mi az adatkezelés jogalapja? Ismertesse az adatkezelés jogalapját (hozzájárulás, szerződés teljesítése, jogi kötelezettség teljesítése, létfontosságú érdekek védelme stb.)* *A gyűjtött adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak-e, valamint a szükségesre korlátozódnak-e (adattakarékosság)? Mutassa be, hogy az egyes gyűjtött adatok miért szükségesek az adatkezelés céljára.* *Pontosak-e az adatok, naprakész állapotban tartják-e azokat? Ismertesse az adatminőséget biztosító intézkedéseket.* *Mi az adatmegőrzés időtartama? Mutassa be, hogy milyen jogi követelmények és/vagy adatkezelési szükségletek indokolják a tárolás időtartamát.*

5. Az érintettek jogainak biztosítása:

Milyen módon tájékoztatják az érintetteket az adatkezelésről? Ismertesse az érintetteknek adott tájékoztatást és annak módját.

Amennyiben az adatkezelés hozzájáruláson alapul, milyen módon szerzik be az érintettek hozzájárulását? Mutassa be az annak biztosítására szolgáló eljárásokat, hogy az érintettek hozzájárulásának beszerzése megtörténik.

Milyen módon érvényesíthetik az érintettek a hozzáférési, illetve az adathordozhatósághoz való jogukat? Ismertesse azokat az intézkedéseket, amelyek biztosítják, hogy az érintettek hozzáférhessenek az adataikhoz, megkapják és továbbíthassák azokat.

Hogyan gyakorolhatják az érintettek a helyesbítéshez és törléshez való jogukat? Ismertesse azokat az intézkedéseket, amelyek biztosítják, hogy az érintettek helyesbíttethessék és töröltethessék adataikat.

Hogyan gyakorolhatják az érintettek az adatkezelés korlátozásához, valamint tiltakozáshoz való jogukat? Ismertesse azokat az intézkedéseket, amelyek biztosítják, hogy az érintettek kérhessék az adatkezelés korlátozását, illetve tiltakozhassanak személyes adataik kezelése ellen.

Az adatfeldolgozók kötelezettségeit egyértelműen rögzíti-e az adatfeldolgozási szerződés? Ismertesse az egyes adatfeldolgozók kötelezettségeit (időtartam, hatás, célok, utasítások a feldolgozóknak, stb.) illetve jelölje meg azok feladatait és kötelezettségeit meghatározó szerződéseket, magatartási kódexeket, és tanúsítványokat.

Az Európai Unión kívülre történő adattovábbítás esetén megfelelő védelemben részesülnek-e a személyes adatok? Nevezze meg mindazokat az EU-n kívüli országokat, amelyekben adatkezelés és adattárolás történik, továbbá jelölje meg, hogy azok megfelelő védelmi szintet biztosítanak-e (más esetben is írja le az adattovábbításra vonatkozó rendelkezéseket.)

6. Kockázatok, tervezett vagy meglévő intézkedések:

Tervezett vagy meglévő intézkedések az adatkezelésből adódó kockázatok mérséklése érdekében.

Logikai biztonságvédelem

Titkosítás
Anonimizálás
Az adatok különválasztása
Logikai hozzáférés szabályozás
Nyomon követhetőség (naplózás)
Archiválás
Papír alapú dokumentumok biztonsága
Adatminimalizálás

Fizikai biztonságvédelem

Üzembiztonság
Rosszindulatú szoftverek kiszűrése
A munkaállomások kezelése
Webhelybiztonság
Biztonsági mentés
Karbantartás
Adatfeldolgozók igénybevétele során alkalmazandó követelmények
Hálózatbiztonság
Fizikai hozzáférésvédelem
Hálózati tevékenységek megfigyelése
Hardverbiztonság
A kockázatforrások elkerülése
A nem emberi eredetű kockázatokkal szembeni védelem

Szervezeti védelmi intézkedések

Szervezet
Szabályzatok
Adatvédelmi kockázatok kezelése
Az adatvédelem beépítése a projektekbe
A személyes adatokkal kapcsolatos jogsértések kezelése
Humánerőforrás-menedzsment
Kapcsolat harmadik felekkel
Felügyelet

7. Kockázatok, jogosulatlan hozzáférés, megváltoztatás, adatvesztés:

Az adatokhoz való jogosulatlan hozzáférés
Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?
Mely fő fenyegető veszélyek idézhetik elő a kockázatot?
Melyek a kockázat forrásai?
A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?
Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)
Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

Az adatok véletlen vagy jogellenes megváltoztatása
Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?
Mely fő fenyegető veszélyek idézhetik elő a kockázatot?
Melyek a kockázat forrásai?
A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?
Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

Adatvesztés
Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?
Mely fő fenyegető veszélyek idézhetik elő a kockázatot?
Melyek a kockázat forrásai?
A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?
Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)
Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel? (elhanyagolható, korlátozott, jelentős, maximális)

8. Adatvédelmi tisztviselő véleménye:

Adatvédelmi tisztviselő véleménye, esetleges korrekciós javaslatok.

9. Az érintettek véleménye:

Az érintettek véleményének kikérése megtörtént-e, és ha nem, akkor miért nem?

Mi volt az érintettek véleménye? Vélemények összegyűjtésének és elemzésének módja.

10. Az Adatkezelő szervezeti egység:

Adatvédelmi tisztviselő jóváhagyása, esetleges korrekciós javaslatok.

Az Adatkezelő szervezeti egység vezetője igazolja, hogy
- *az adatkezelés körülményeinek a leírása megfelel a valóságnak.*
- *a kockázatokat a tervezett és meglévő intézkedések szerint vette tekintetbe.*

Jóváhagyja a jelzett korrekciós intézkedéseket.
Vállalja a jelzett korrekciós intézkedések mihamarabbi megvalósítását.

Érdekmérlegelési teszt
(minta)

1. Az érdekmérlegelési teszt elvégzésének oka:
Annak bemutatása, hogy a személyes adatok kezelése elengedhetetlen a cél elérése érdekében: - *igazolni és dokumentálni szükséges, hogy nincs olyan alternatív megoldás, amely személyes adatok kezelése nélkül alkalmas lenne a cél elérésére* *Annak bemutatása, hogy a GDPR 6. cikk (1) bekezdése a)- f) pontjai közül kizárólag az f) pont, azaz a jogos érdek képezi az adatkezelés alapját:* - *igazolni és dokumentálni szükséges, hogy a jogalapok közül, kizárólag a jogos érdek alkalmazható*

2. A Társaság, mint adatkezelő jogos érdeke:
A kellően konkrét jogos érdek bemutatása: - *azon jogszabályhelyek felsorolása, amelyek lehetővé és nem kötelezővé teszik az adatkezelést (jogi érdek),* - *társadalmi-, üzleti-, gazdasági érdekek kifejtése.*

3. Az adatkezelés célja, milyen személyes adatok, mennyi ideig tartó adatkezelését igényli a jogos érdek:
Az adatkezelés célja: *A kezelt személyes adatok köre:* *Adatkezelés időtartama:*

4. Az Érintett érdekei, alapjogok:
Az Érintettek, mint természetes személynek jogszabályokon (GDPR, Alaptörvény, Infotv, Ptk., stb.) alapuló, az adatkezeléssel érintett, védelmet élvező érdekének, jogosultságainak meghatározása. *Az Érintettnek, mint természetes személynek az előbbiek szerinti védelmet élvező érdeke fűződik ahhoz, hogy:* - *információs önrendelkezési jogát gyakorolhassa,* - *saját személyes adatainak mások általi kezeléséről maga rendelkezhessen,* - *magánszféráját az adatkezelők tiszteletben tartsák,* - *az információs önrendelkezési jog érvényesítését elősegítő, illetve a személyes adatok és ezen keresztül a magánszféra védelmét biztosító jogszabályi rendelkezések érvényesüljenek.* *Az adatkezelésből eredő, Érintettre kiható azon következmények összegyűjtése, amelyek az Érintett érdekeit szolgálják, rá nézve pozitív hatásként jelentkeznek.*

5. A Társaság jogos érdekeinek és az Érintettek érdekeinek, alapjogainak súlyozása:
Súlyozás a 2-es és 4-es pont összevetésével.

6. A biztosítékok, garanciák:
Mindazoknak a biztosítékoknak és garanciáknak a felsorolása, melyek az adatkezelés alapelveinek érvényesülését elősegítik, továbbá annak alátámasztása, hogy az érintett adatkezeléssel kapcsolatban felmerült érdekeinek, jogainak korlátozása a szükségesség, arányosság elvének érvényesülése mellett történt. Érintetti jogok biztosítására hozott intézkedések: *Az érintetti jogok (pl.: előzetes tájékoztatás, hozzáférési jog, tiltakozás, helyesbítés) biztosítására hozott intézkedések kifejtése, az átláthatóság elvének érvényesülése érdekében.* Biztonsági intézkedések: *Azoknak a technikai és szervezési intézkedéseknek a kifejtése, amelyek az adatok biztonságos kezelését garantálják.* Jogorvoslati lehetőségek feltüntetése: *Belső- és külső csatornák feltüntetése. (Adatvédelmi tisztviselő, bíróság, hatóság)*

7. Az érdekmérlegelési teszt eredménye:
A fent kifejtettek összefoglalása, az érdekmérlegelési teszt végeredményeképpen az adatkezelő jogos érdeke vagy az érintett jogos érdeke elsőbbségének meghatározása, az eredmény dokumentálása.

Belső adatvédelmi nyilvántartásba bejelentő lap

…….

(adatkezelési tevékenység megnevezése)

Iktatószám: .....

1. Azonosító adatok *(Adatvédelmi tisztviselő tölti ki)*

1.1 Sorszám:	
1.2 Belső adatvédelmi nyilvántartásba vétel dátuma:	

2. Adatkezelő szervezeti egység *(Adatkezelő szervezeti egység tölti ki)*

2.1 Megnevezése:	
2.2 Címe:	
2.3 Telefonszáma / email címe:	
2.4 Kapcsolattartó neve:	
2.5 Kapcsolattartó elérhetőségei:	

3. Közös adatkezelő adatai *(Adatkezelő szervezeti egység tölti ki)*

3.1 Megnevezése:	
3.2 Címe:	
3.3 Telefonszáma / email címe:	
3.4 Adatvédelmi tisztviselő neve:	
3.5 Adatvédelmi tisztviselő elérhetőségei:	

4. Adatfeldolgozó adatai *(Adatkezelő szervezeti egység tölti ki)*

4.1 Megnevezése:	
4.2 Címe:	
4.3 Telefonszáma / email címe:	
4.4 Adatvédelmi tisztviselő neve:	
4.5 Adatvédelmi tisztviselő elérhetőségei:	

5. Az adatkezelés paraméterei *(Adatkezelő szervezeti egység tölti ki)*

5.1 Adatkezelés célja:	
5.2 Kezelt adatok köre:	
5.3 Adatok forrása:	
5.4 Személyes adatok kezelésére vonatkozó hivatkozás, szabályozás, utasítás:	
5.5 Érintettek köre:	
5.6 Ki férhet hozzá az adatokhoz	
5.7 Adatkezelés időtartama	
5.8 Adatkezelés jogalapja	
5.9 Tájékoztató típusa	

6. Az adattovábbítás címzettjei *(Adatkezelő szervezeti egység tölti ki)*

6.1 Megnevezése:	
6.2 Címe:	
6.3 Telefonszáma / email címe:	
6.4 Adatvédelmi tisztviselő elérhetőségei:	
6.5 Harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás esetén, az arra vonatkozó információk, garanciák:	

7. Tárolás *(Adatkezelő szervezeti egység tölti ki)*

8.1 Adathordozó típusa:	
8.2 Tárolás helye:	

8. Adatkezelés megszüntetése *(Adatkezelő szervezeti egység tölti ki)*

9.1 Törlés / anonimizálás dátuma:	

Adatkezelési tájékoztató

…….

(*adatkezelési tevékenység megnevezése***)**

1. Az adatkezelő megnevezése

Név:	MÁV-START Vasúti Személyszállító Zártkörűen Működő Részvénytársaság
Székhely:	1087 Budapest, Könyves Kálmán krt. 54-60.
Cégjegyzékszám:	01-10-045551
Adószám:	13834492-2-44
E-mail:	.....*@mav-start.hu*
a továbbiakban:	Adatkezelő.

Adatvédelmi tisztviselő elérhetőségei:
E-mail: adatvedelem@mav-start.hu
Postai cím: 1087 Budapest, Könyves Kálmán krt. 54-60. – a borítékon kérjük megjelölni a következőket: „Adatvédelmi tisztviselő részére”.

2. Adatfeldolgozó megnevezése

Név:	……..
Székhely:	……..
Cégjegyzékszám:	……..
Adószám:	……..
E-mail:	……..
a továbbiakban:	Adatfeldolgozó.

Az Adatkezelő és az Adatfeldolgozó közötti viszony részletezése, az adatfeldolgozás megjelölése.

3. Az érintett személye: valamennyi természetes személy, aki ……. (a továbbiakban: érintett). *Az érintett személyének pontos meghatározása.*

4. Az adatkezelésre vonatkozó információk

4.1. Az adatkezelés célja: *az adatkezelés céljának pontos, konkrét és érthető kifejtése. Amennyiben az adatkezelésnek több egymástól független célja van, úgy az adatkezelési tájékoztatóban e célokat egymástól jól elkülönítetten szükséges megjelölni és a 4.2. – 4.8. pontokban foglalt információkat minden adatkezelési cél tekintetében rögzíteni kell.*
4.2. Az adatkezelés jogalapja: *a személyes adatok esetén a GDPR 6. cikk (1) bekezdés a) – f) pontja szerinti jogalap, valamint különleges adatok esetén a GDPR 9. cikk (2) bekezdés szerinti többletfeltétel megjelölése szükséges. Amennyiben az adatkezelés jogalap a GDPR 6. cikk (1) bekezdésének f) pontja, úgy a jogos érdek rövid kifejtése is szükséges.*
4.3. A kezelt adatok köre: *a kezelt adatok körének megjelölése, szükség esetén az egyes személyes adatok kezelésének célja(i).*
4.4. Az adatkezelés időtartama: *az adatkezelés időtartamának pontos megjelölése, vagy az adatkezelés időtartamának meghatározására alkalmas szempontok ismertetése.*
4.5. Az adatkezelés módja: *annak megjelölése, hogy a személyes adatok kezelése papír alapon vagy elektronikus úton történik. Amennyiben az adatkezelés során automatizált döntéshozatalra vagy profilalkotásra kerül sor, úgy ennek tényének megjelölése szükséges, valamint legalább ezekben az esetekben az alkalmazott logika és arra vonatkozóan érthető információ(k), hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.*

***4.6. Az adatok forrása**: annak megjelölése, hogy az adatkezelő milyen forrásból szerzi meg a személyes adatokat (pl. az érintettől vagy más adatkezelőtől).*
***4.7. Az adatok megismerésére jogosultak köre:** azon személyi kör megjelölése, akik jogosultak a személyes adatok megismerésére.*
***4.8. A személyes adatok szolgáltatásának kötelezettsége és az adatszolgáltatás elmaradásának következménye:** annak ismertetése, hogy a személyes adatokat az érintett köteles-e rendelkezésre bocsátani, illetve ha igen, úgy az adatszolgáltatás elmaradása következményeinek ismertetése.*

5. Adatbiztonsági intézkedésekről szóló tájékoztatás

Az adatkezelés során alkalmazott adatbiztonsági intézkedések ismertetése.

6. Az érintettek jogai és jogérvényesítési lehetőségei

Az érintetteket megillető jogosultságok megjelölése és azok adatkezelési folyamat keretében való érvényesülésének kifejtése. Az érintettet minden esetben megilleti: az előzetes tájékoztatáshoz való jog, a hozzáféréshez való jog (annak minden részjogosultságával), a helyesbítéshez való jog (abban az esetben, ha az adatkezelés körülményeire tekintettel e jog értelmezhető), törléshez való jog, az adatkezelés korlátozásához való jog, jogorvoslathoz való jog (panasztételhez való jog és bírósághoz való fordulás joga). Az érintettet az alábbi jogok illethetik meg (az adatkezelés jogalapjának és egyéb körülmények függvényében): adathordozhatósághoz való jog, a hozzájárulás visszavonásának joga, tiltakozáshoz való jog. A panasztételhez való jogról szóló tájékoztatás keretében az adatvédelmi felügyeleti hatóság valamennyi elérhetőségét közölni kell.

7. Az adatkezelés tekintetében releváns jogszabályok

- 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 (általános adatvédelmi rendelet vagy GDPR),
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.)

E pont keretében meg kell jelölni az adatkezelés tekintetében irányadó további jogszabályokat.

MÁV-START Zrt.
Adatkezelő

Adatvédelmi Incidens nyilvántartás

sorszám	
incidens bejelentésének, feltárásának időpontja	
incidens bekövetkezésének vélelmezett időpontja	
érintett személyes adatok köre	
incidenssel érintettek köre	
incidenssel érintettek száma	
incidens jellege és körülményei	
incidens hatásai	
incidens elhárításra tett intézkedések	
incidens elhárítá-sának időpontja	
az adatkezelést előíró jogszabály-ban meghatáro-zott egyéb adatok	
érintett szervezeti egység	

ügyintéző/vizsgáló neve, elérhetősége	
kapcsolódó dokumentumok	
hatósági /fegyelmi eljárás, következmény, ennek adatai	
különleges adatot tartalmaz (I/N)	

MÁV-START	**MEGBÍZÁS BELSŐ ADATVÉDELMI AUDITORI TEVÉKENYSÉG ELVÉGZÉSÉRE**

Név, beosztás: ……., adatvédelmi tisztviselő
A megbízás érvényessége:
A megbízás célja:
A feladat ellátásával összefüggésben felmerülő esetleges költségek viselése:
Feladat, hatáskör és felelősség:

……
(név)
(beosztás)

A megbízás eredeti példányát átvettem,

dátum:
aláírás:

Iktatószám: ...../...../START

Feljegyzés
az érintett által szóban előterjesztett érintetti jogok gyakorlásával összefüggő kérelemhez

I. Érintetti jogot gyakorló személy adatai:[1]

Név: …….
Születési hely és idő: ……...
Anyja neve: ……..
Kapcsolattartási adatok (legalább az egyik):
E-mail cím: …….....
Postai cím: …….....
Egyéb azonosításhoz szükséges adat (amennyiben az adatkezelés jellege további adat megadását teszi szükségessé): …….....

II. Az érintett által előadottak (bővíthető):

.....

.....

.....

.....

.....

III. A kérelem előterjesztésének napja:

.....

IV. A kérelmet rögzítő neve, munkaköre:

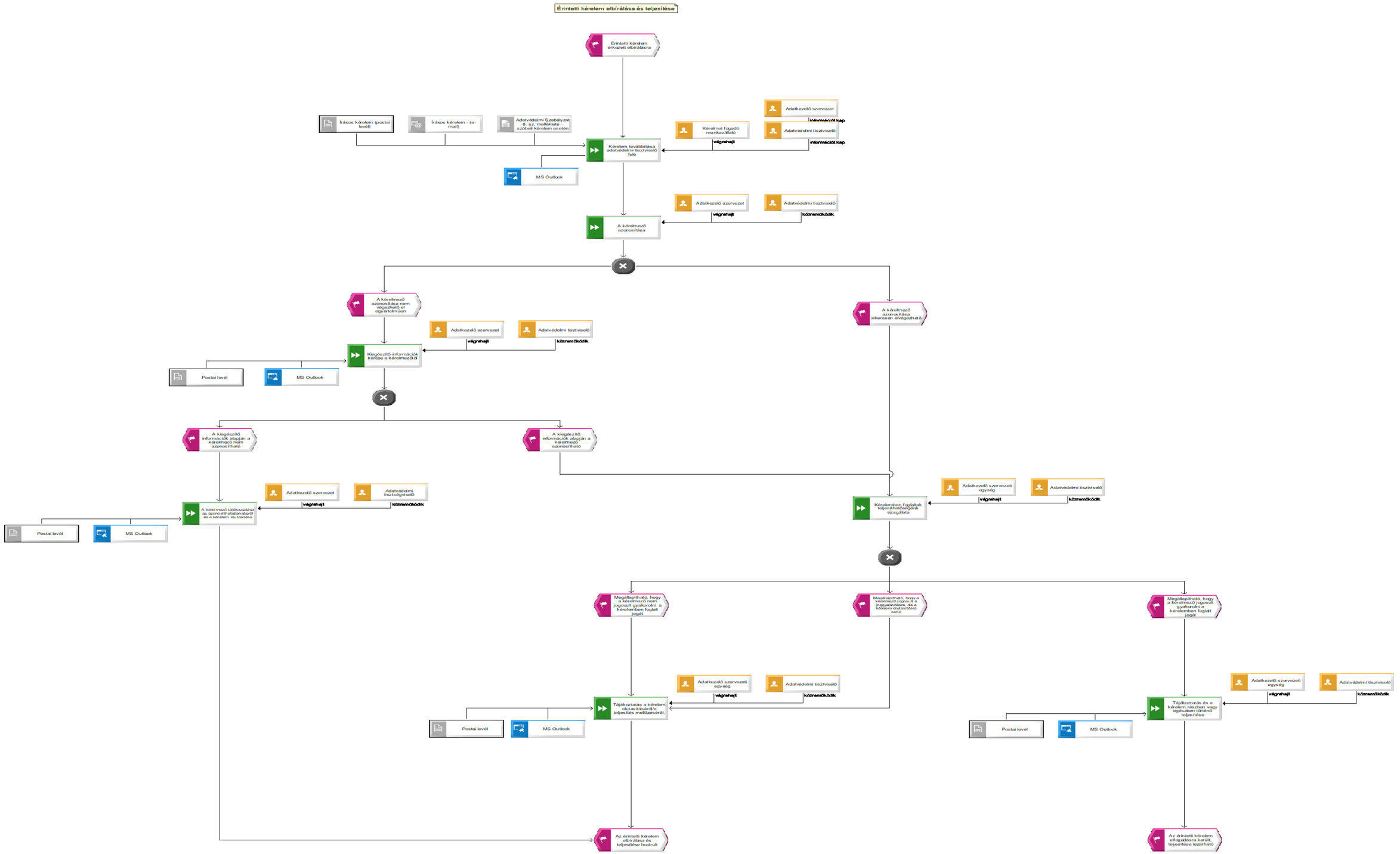
.....

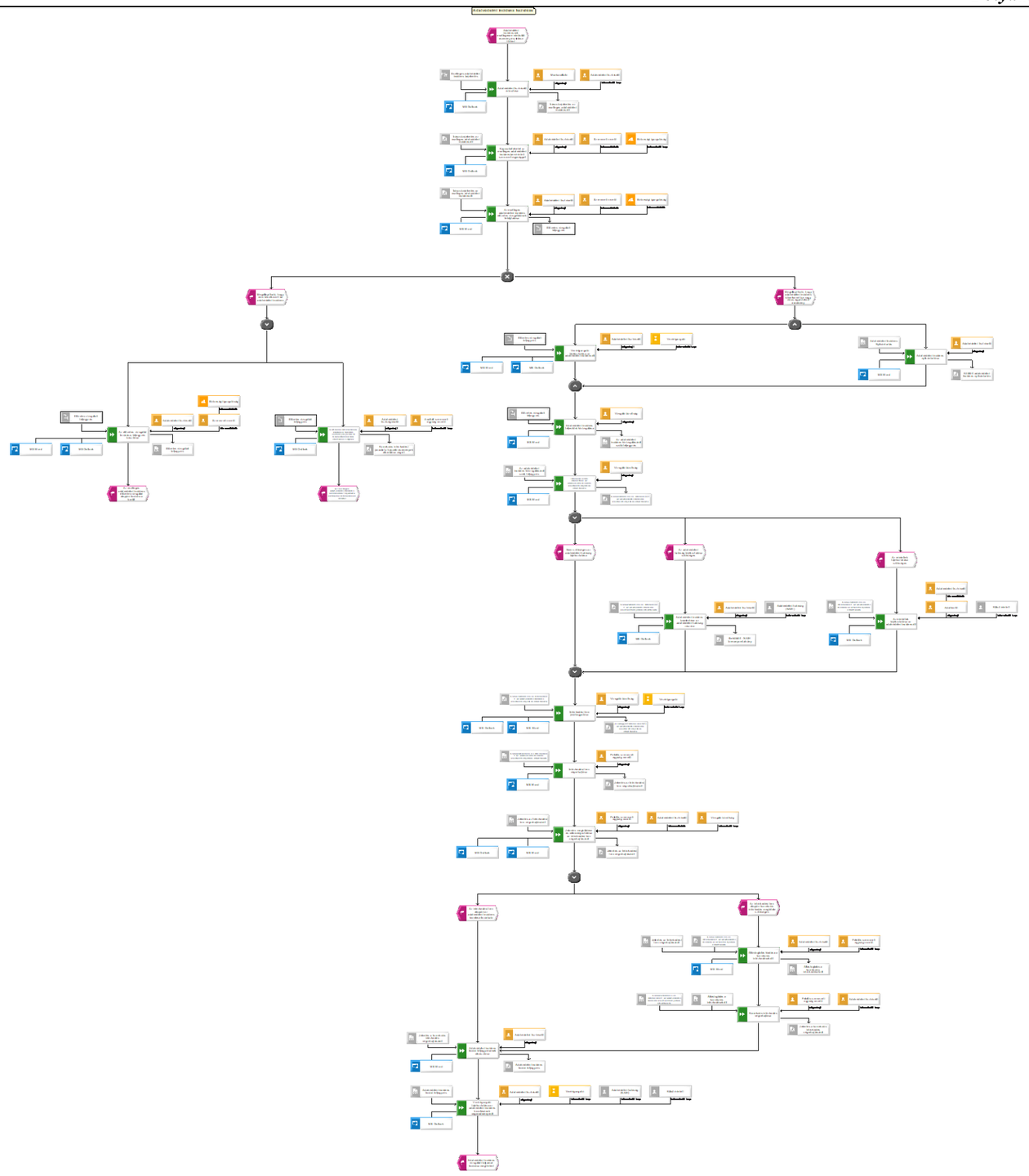
V. A kérelem belső továbbításával kapcsolatos adatok:

V.1. Az adatvédelmi tisztviselő részére történő továbbításának napja: …….....
V.2. Az adatkezelő szervezeti egység részére történő továbbítás napja: …….....

……..……
A feljegyzést készítő aláírása

[1] Az adatkezelési tájékoztató a https://www.mavcsoport.hu/mav-start/bemutatkozas/adakezelesi-tajekoztatok honlapon, a 4.1. pont alatt érhető el.


Érintetti kérelem elbírálása és teljesítése
Érintetti kérelem érkezett elbírálásra
Írásos kérelem (postai levél)
Írásos kérelem - (e-mail)
Adatvédelmi Szabályzat 8. sz. melléklete - szóbeli kérelem esetén
Kérelmet fogadó munkavállaló
Adatkezelő szervezet
Adatvédelmi tisztviselő
információt kap
végrehajt
információt kap
Kérelem továbbítása adatvédelmi tisztviselő felé
MS Outlook
Adatkezelő szervezet
Adatvédelmi tisztviselő
végrehajt
közreműködik
A kérelmező azonosítása
A kérelmező azonosítása nem végezhető el egyértelműen
A kérelmező azonosítása sikeresen elvégezhető.
Adatkezelő szervezet
Adatvédelmi tisztviselő
végrehajt
közreműködik
Kiegészítő információk kérése a kérelmezőtől
Postai levél
MS Outlook
A kiegészítő információk alapján a kérelmező nem azonosítható
A kiegészítő információk alapján a kérelmező azonosítható
Adatkezelő szervezet
Adatvédelmi tisztségviselő
végrehajt
közreműködik
A kérelmező tájékoztatása az azonosíthatatlanságról és a kérelem elutasítása
Postai levél
MS Outlook
Adatkezelő szervezeti egység
Adatvédelmi tisztviselő
végrehajt
közreműködik
Kérelemben foglaltak teljesíthetőségének vizsgálata
Megállapítható, hogy a kérelmező nem jogosult gyakorolni a kérelemben foglalt jogát
Megállapítható, hogy a kérelmező jogosult a kérelemre, de a kérelem elutasítására kerül
Megállapítható, hogy a kérelmező jogosult gyakorolni a kérelemben foglalt jogát
Adatkezelő szervezeti egység
Adatvédelmi tisztviselő
végrehajt
közreműködik
Tájékoztatás a kérelem elutasításáról/a teljesítés mellőzéséről.
Postai levél
MS Outlook
Tájékoztatás és a kérelem részben vagy egészben történő teljesítése
Adatkezelő szervezeti egység
Adatvédelmi tisztviselő
végrehajt
közreműködik
Postai levél
MS Outlook
Az érintetti kérelem elbírálása és teljesítése lezárult
Az érintetti kérelem elfogadásra került, teljesítése lezárható



Szerkeszti: MÁV-START Zrt. Kabinet

Felelős kiadó: Keresztes Péter vezérigazgató