ÉRTESÍTŐ

2019/30. SZÁM

TARTALOM

30. szám Budapest, 2019. július 18.

Utasítások

45/2019. (VII. 18. MÁV-START Ért. 30.) sz. vezérigazgatói utasítás az Adatvédelmi Szabályzatról

1.0 AZ UTASÍTÁS CÉLJA

Az utasítás célja, hogy meghatározza a MÁV-START Zrt. (a továbbiakban: Társaság) tevékenységével összefüggésben a Társaság birtokába kerülő személyes adatok kezelésének- és azok nyilvántartásának rendjét, illetve megteremtse a személyes adatok szabad áramlásához szükséges feltételeket, a vonatkozó jogi szabályozás tükrében.

Fentiek teljesülése érdekében jelen utasítás a Társaság adatvédelmi szabályozási struktúrájának tetején foglal helyet. Jelen utasítás rendelkezéseit figyelembe kell venni a Társaságnál kiadásra kerülő szabályozások kialakításakor, illetve meglévő (hatályos) szabályozások módosításakor.

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.

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

Az utasítás elkészítéséért és szükség szerinti módosításáért a Társaság Biztonsági Igazgatója felelős, az Adatvédelmi tisztviselővel egyetemlegesen.

Az utasításban előírtak betartatásáért a feladatkörében minden érintett szervezeti egység vezetője felelős.

A személyes adatok kezelésének megtervezésekor figyelemmel kell lenni arra, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

A Társaság munkatársai munkájuk során kötelesek gondoskodni arról, hogy jogosulatlan személyek ne férhessenek hozzá személyes adatokhoz.

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.

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 azon SZMSZ szerinti szervezeti egysége, amely az adatkezelést a Társaság képviseletében végzi.

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

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

Az adatvédelmi munkacsoport: a Társaság adatkezelő szervezeti egységeinek munkatársaiból áll. A munkacsoport tagok feladata az adatvédelmi megfelelés elősegítése, illetve kapcsolattartás az őt delegáló szervezeti egység és az adatvédelmi tisztviselő között. A munkacsoporttagokat az adatkezelő delegálja, azon munkavállalói közül, akik ismerik a szervezet által végzett munkafolyamatokat.

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

Adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése 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.

Adattörléshez való jog („elfeledtetéshez való jog"): Az érintett joga arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, jogszabályban meghatározott esetekben.

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.

Adatvédelem: a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozását, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

Adatvédelmi szakértők (DPO munkatársai): Az adatvédelmi tisztviselő közvetlen irányítása alatt álló szakértő(k), akik segítik a szervezeti egységek és az adatvédelmi tisztviselő munkáját a szükséges dokumentumok, folyamatok előkészítésével.

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.

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.

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

GDPR: 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.

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 EGT-állam.

Hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság, mely független szervként a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését ellenőrzi.

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 kategóriái: 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.

Szűkített adatvédelmi munkacsoport: az adatvédelmi munkacsoport tagjai közül az adatkezelő szervezeti egység vezetője által delegált munkavállaló.

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

4.0 AZ UTASÍTÁS LEÍRÁSA

A Társaság (köz)szolgáltatói- és üzleti szereplőként tevékenységi körében különösen utasainak-, ügyfeleinek-, partner vasúttársaságok munkavállalóinak- és azok családtagjainak, továbbá üzleti partnereinek jelentős mennyiségű személyes adata kezeléséért felelős.

A Társaság, mint munkáltató kezeli a munkavállalóinak- és azok családtagjainak személyes adatait is.

Személyes adat kezelésére csak jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség. A Társaság által kezelt személyes adatok magáncélra való felhasználása tilos. Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének.

A Társaság szervezeti egységeinél adatkezelést végző munkavállalók és a Társaság megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek munkavállalói kötelesek a megismert személyes adatokat megőrizni. A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek Titoktartási nyilatkozatot tenni. Ha az Utasítás hatálya alatt álló személy tudomást szerez arról, hogy a Társaság által kezelt személyes adat hibás, hiányos vagy időközben megváltozott, haladéktalanul köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni. Az adatvédelmi jogszabályoknak való megfelelés érdekében a Társaságnak

- alkalmaznia kell egy fő Adatvédelmi tisztviselőt,
- az adatkezeléseit úgy kell megterveznie, hogy azok megfeleljenek az adatvédelem alapelvének,
- a személyes adatok kezelése alapelveinek az adatkezelés teljes folyamatában érvényesülniük kell, valamint
- az adatkezelés teljes folyamatának leteltével, az adatkezelés céljának megvalósulásával, a személyes adatokat törölni, vagy anonimizálni kell.

A személyes adatkezelés, adatfeldolgozás során az abban résztvevők között – különösen az Adatvédelmi tisztviselő és az Adatkezelő, valamint az Adatvédelmi tisztviselő és az adatvédelmi munkacsoport tagjai között – a kommunikáció (pl. tájékoztatás, tanácsadás) generális szabályként írásban történik (ideértve az elektronikus levelezést is).

4.1 A személyes adat kezelésének általános szabályai

Az utasítás jelen szakasza, a 4.1-es pont a Társaság, mint adatkezelő legfontosabb feladatait általánosságban írja le. Ezek a feladatok a konkrét adatkezeléssel járó folyamatok tekintetében automatikusan delegálásra kerülnek az adott adatkezelő szervezeti egység felelősségi és feladatkörébe. Az adatkezelő szervezeti egységek konkrét feladatai a 4.2-es ponttól a 4.4-es pontig kerülnek kifejtésre. Ezen pontok helyenként visszautalnak az utasítás általános részéhez, de a feladatok és felelősségek továbbra is az adott folyamatért felelős adatkezelő szervezeti egységet terhelik.

4.1.1 A személyes adatok kezelésének alapelvei

A személyes adatok kezelésének minden szakaszában érvényesülnie kell, az alábbi alapelveknek.

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.

A ***célhoz kötöttség*** elvének megfelelően a Társaság személyes adatot csak meghatározott, jogszerű célból, jog gyakorlása vagy kötelezettség teljesítése érdekében kezelhet, a cél eléréséhez szükséges minimális mértékben és ideig. Az adatkezelés minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatokat törölni kell.

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.

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

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.

Az ***integritás és bizalmas jelleg*** elvének megfelelően az Adatkezelő az adatkezelést úgy alakítja ki, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága. Gondoskodnia kell az adatok jogosulatlan vagy jogellenes kezelésének megakadályozásáról, illetve biztosítania kell a véletlen elvesztés, megsemmisítés vagy károsodás elleni védelmet.

Az ***elszámoltathatóság*** elvének való megfelelés keretében a Társaságra hárul annak felelőssége, hogy a fent felsorolt elveknek megfeleljen az adatkezelés teljes folyamata, ebből adódóan a Társaságnak képesnek kell lennie a megfelelőség igazolására. A megfelelőség igazolása érdekében a Társaság az adatkezeléssel járó szakmai folyamatait érintő belső utasításaiban ki kell, hogy térjen az adatok kezelésével kapcsolatos valamennyi körülményre.

4.1.2 A személyes adatok kezelésének jogalapjai

A Társaságnál személyes adat csak a GDPR 6. cikk (1) bekezdésében foglaltak alapján, míg a személyes adatok különleges kategóriájába tartozó személyes adat csak a GDPR 9. cikkben foglaltak alapján, az alábbiak szerint kezelhető.

4.1.2.1 A személyes adatok kezelésének jogalapjai

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 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 járhat. A hozzájárulást az adatkezelőtől kapott konkrét, és megfelelő tájékoztatásnak kell megelőznie.

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, a hozzájárulási nyilatkozatot egyértelműen el kell különíteni az egyéb tartalomtól, nyelvezetének egyszerűnek és világosnak kell lennie.

Az Adatkezelőnek az érintett hozzájárulását adatkezelési célonként kell elkérnie. Ha egy adatkezelésnél több adatkezelési célt szükséges megjelölni, akkor az Adatkezelőnek úgy kell kialakítania a hozzájáruló nyilatkozatot, hogy az érintett célonként külön-külön tudja megadni hozzájárulását.

Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely nincs összhangban a GDPR rendelkezéseivel, kötelező erővel nem bír.

Az érintett hozzájárulását bármikor visszavonhatja, erre az adatkezelőnek egyszerű lehetőséget kell biztosítania. 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 16. életévét betöltött kiskorú gyermek, mint érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezeléséhez szülői hozzájárulás, illetve engedély szükséges, *kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló személy adta meg, illetve engedélyezte.*

Szerződés teljesítése

Az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben 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, üzleti partnerei, munkavállalói közt létrejött szerződés keretében megvalósuló, vagy ahhoz kapcsolódó személyes adatkezelések esetén alkalmazandó.

Jogi kötelezettség teljesítése
Az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. Ezt az adatkezelő elsősorban akkor alkalmazhatja, ha az adatok kezelését jogszabály kifejezetten előírja, vagy ha az érintett(ek) jogaira nézve megfelelő garanciákról rendelkező jogszabály lehetőséget biztosít annak alkalmazására.

Az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme
Az adatkezelés az érintett vagy másik természetes személy létfontosságú érdekeinek védelmében történik. Ez az adatkezelési jogalap elvben csak akkor alkalmazható, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető.

Közérdekű feladat végrehajtása
Az adatkezelés ***közérdekű*** vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges. Ebben az esetben az adatkezelésnek jogszabályban foglalt jogalappal kell rendelkeznie.

Jogos érdek érvényesítése
Az adatkezelés az adatkezelő vagy egy harmadik fél ***jogos érdek***einek érvényesítéséhez szükséges. Fontos kitétel, hogy ezen jogalap alkalmazása csak akkor lehetséges, ha az adatkezelő vagy harmadik fél jogos érdekei elsőbbséget élveznek az érintett érdekei vagy alapvető jogai és szabadságaival szemben, amelyek személyes adatok védelmét teszik szükségessé. Az adatkezelő a jogos érdek alátámasztása érdekében érdekmérlegelési tesztet végez.

A jogi kötelezettség teljesítése, illetve a közérdekű vagy közhatalmi jogosítvány alapján megvalósuló adatkezelés jogalapját uniós-, vagy hatályos tagállami jognak kell megállapítania.

4.1.2.2 Személyes adatok különleges kategóriái

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 valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;
- 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.

4.1.2.3 A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése

A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok kezelésére kizárólag abban az esetben kerülhet sor, ha az adatkezelést az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó jogszabály lehetővé teszi.

4.1.3 Érintettek jogainak biztosítása

A Társaságnak a személyes adatok kezelésének teljes szakaszában biztosítania kell az érintetti jogok gyakorolhatóságát.

4.1.3.1 Általános szabályok

A Társaságnak úgy kell megvalósítania az érintett tájékoztatását, hogy az érintett részére a személyes adatok kezelésére vonatkozó tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. A tájékoztatás nyelvezetének mindig igazodnia kell az érintettek köréhez. A tájékoztatást írásban vagy egyéb, megtörténtének bizonyítására alkalmas módon kell biztosítani.

A Társaságnak az adatkezelést úgy kell kialakítania, hogy adott esetben biztosítható legyen az érintett hozzáférési-, helyesbítéshez és törléshez való-, az adatkezelés korlátozásához való-, az adathordozhatósághoz való-, a tiltakozáshoz való-, és az automatizált döntéshozatallal kapcsolatban felmerülő jogainak gyakorolhatósága.

A Társaságnak az érintettek kérelmére indokolatlan késedelem nélkül, a kérelem kézhezvételétől számított egy hónapon belül tájékoztatnia kell az érintettet a kérelme nyomán megtett intézkedésekről. A határidő a kérelem összetettségére és a kérelmek számára való tekintettel, egy alkalommal legfeljebb további két hónappal meghosszabbítható. Az érintettet a kézhezvételtől számított egy hónapon belül tájékoztatni kell a meghosszabbítás tényéről és annak okáról.

A Társaságnak, a kérelem elektronikus úton történő beérkezése esetén, elsősorban elektronikus úton kell azt megválaszolnia, amelytől eltérni akkor lehet, ha az érintett azt kifejezetten másként kéri. A megválaszolás tényének azonban minden esetben bizonyíthatónak kell lennie.

Ha a Társaság nem tesz intézkedéseket az érintett kérelme nyomán, úgy késedelem nélkül, de legkésőbb a kérelem kézhezvételétől számított egy hónapon belül tájékoztatnia kell az érintettet az intézkedés elmaradásának okairól, valamint a bírósági jogorvoslat-, illetve a Hatósághoz fordulás lehetőségéről.

A Társaságnak az érintett tájékoztatását és jogainak gyakorlását díjmentesen kell biztosítania. Ez alól kivételt jelent, ha az érintett kérelme egyértelműen megalapozatlan, vagy – különösen ismétlődő jellege miatt – túlzó. Ebben az esetben a Társaság figyelemmel az adminisztratív költségekre, észszerű összegű díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő intézkedést. A megalapozatlan vagy túlzó jelleg bizonyítása a Társaságot terheli. A megalapozatlan vagy túlzó jelleget egyedileg kérelmenként kell megállapítani. Túlzó jellegű lehet a kérelem, ha folyó évben azonos adatkörre vonatkozóan az érintett már nyújtott be kérelmet. A már megfizetett költségtérítést a Társaság vissza kell, hogy térítse, amennyiben az adatokat jogellenesen kezelte, vagy a tájékoztatás kérése helyesbítéshez vezetett.

Az érintetti jogok biztosítása során felmerülő költségtérítés megállapításának folyamata:

- A Társasághoz beérkezett igényt az azt fogadó szervezeti egység haladéktalanul köteles továbbítani az Adatvédelmi tisztviselő és az érintett Adatkezelő szervezeti egység részére.
- A Társaság Adatkezelő szervezeti egységének – figyelemmel a személyes adatok kezelésére vonatkozó alapelvekre – mérlegelnie kell, hogy a kérés megalapozatlan vagy túlzó jellegű-e, másolatkérési jog teljesítése esetén pedig azt, hogy első alkalommal történik-e az igénylés.
- Amennyiben az igény teljesítésre kerül, a Társaság Adatkezelő szervezeti egységének – figyelemmel a személyes adatok kezelésére vonatkozó alapelvekre – össze kell gyűjtenie a kérés teljesítéséhez szükséges anyagköltséget és ráfordítandó munkaóra költségét.
- A Társaság Adatkezelő szervezeti egységének a kérés teljesítéséhez szükséges adminisztratív költségről tájékoztatnia kell az érintettet.
- Az érintett részéről történő költség elfogadása esetén a Társaság Adatkezelő szervezeti egységének teljesítenie kell az érintett kérését és tájékoztatnia kell az Adatvédelmi tisztviselőt.

Amennyiben a Társaság nem tudja beazonosítani a jogaival élni kívánó érintettet, akkor további, a beazonosításra alkalmas adatokat kell bekérnie tőle.

4.1.3.2 Az érintett tájékoztatása

Az érintett tájékoztatása kétféleképpen történhet:

I. az egyik esetben a Társaság a személyes adatokat közvetlenül az érintettől,
II. a másik esetben nem az érintettől szerzi be.

I. *Ha az érintettre vonatkozó személyes adatok beszerzése közvetlenül az érintettől történik, a Társaságnak a legkésőbb az adatok beszerzésének időpontjában,*

a) tájékoztatnia kell az érintettet:

- a Társaság megnevezéséről valamint kapcsolattartás céljából fenntartott elérhetőségekről,
- az Adatvédelmi tisztviselő elérhetőségeiről,
- az adatkezelés céljáról és jogalapjáról,
- amennyiben az adatkezelés jogos érdeken alapul, a Társaság vagy harmadik fél jogos érdekeiről,
- adattovábbítás esetén, annak címzettjeiről, illetve a címzettek kategóriáiról,
- harmadik országba történő adattovábbítás esetén, annak tényéről, valamint az GDPR-ban meghatározott egyéb körülményeiről.

b) a tisztességes és átlátható adatkezelés elvének való megfelelés érdekében a tájékoztatónak információval kell szolgálnia:

- a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól,
- az érintett azon jogáról, hogy kérelmezheti a Társaságtól a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogának gyakorlásáról,
- a hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jogáról, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
- felügyeleti hatósághoz címzett panasz benyújtásának jogáról,
- arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása,
- automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról és arra vonatkozóan érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Amennyiben a Társaság a személyes adatokat a gyűjtésük céljától eltérő célból kívánja kezelni, az új adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról, továbbá az I/b) pontban jelzett adatkezelési körülményekről.

II. *Ha az érintettre vonatkozó személyes adatok beszerzése nem az érintettől történik, a Társaságnak*

a) tájékoztatnia kell az érintettet:

- a Társaság megnevezéséről valamint kapcsolattartás céljából fenntartott elérhetőségekről,
- az Adatvédelmi tisztviselő elérhetőségeiről,
- az adatkezelés céljáról és jogalapjáról,
- az adatkezelésben érintett személyes adatok kategóriáiról,
- adattovábbítás esetén, annak címzettjeiről, illetve a címzettek kategóriáiról,
- harmadik országba történő adattovábbítás esetén, annak tényéről, valamint az GDPR-ban meghatározott egyéb körülményeiről.

b) továbbá a tisztességes és átlátható adatkezelés érdekében a tájékoztatónak információval kell szolgálnia:

- a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól,
- amennyiben az adatkezelés jogos érdeken alapul, a Társaság vagy harmadik fél jogos érdekeiről,
- az érintett azon jogáról, hogy kérelmezheti a Társaságtól a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról,
- a hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jogáról, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
- felügyeleti hatósághoz címzett panasz benyújtásának jogáról,
- az adatok forrásáról, adott esetben a nyilvános forrásra külön ki kell térni,
- automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról és arra vonatkozóan érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

A Társaságnak az érintett tájékoztatását úgy kell megvalósítania, hogy az a személyes adatok kezelésének konkrét körülményeit figyelembe véve, a személyes adatok megszerzésétől számított ésszerű határidőn, de legkésőbb egy hónapon belül megtörténjen. Ezen a határidőn belül, ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával, illetve ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor kell megadni a tájékoztatást.

Amennyiben a Társaság a személyes adatokat a gyűjtésük céljától eltérő célból kívánja kezelni, az új adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról, továbbá a b) pontban jelzett adatkezelési körülményekről.

A Társaságnak nem kell tájékoztatnia az érintettet, amennyiben

- az információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy
- aránytalanul nagy erőfeszítést igényelne, vagy
- valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné az adatkezelés céljainak elérését.

Előbbi esetekben az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, a Társaságnak megfelelő intézkedéseket kell hoznia, például a tájékoztatás nyilvános elérhetőségének biztosításával.

A Társaság tájékoztatási kötelezettsége szintén nem áll fenn, amennyiben a személyes adat megszerzését, vagy közlését kifejezetten előírja jogszabály, amely az érintett jogos érdekét szolgáló intézkedésekről külön rendelkezik, vagy ha a személyes adatoknak valamely jogszabályban előírt titoktartási kötelezettség alapján bizalmasnak kell maradniuk.

Hatósági ajánlás által támasztott további tájékoztatási kötelezettség

A Hatóság által kibocsátott ajánlás értelmében mind a I., mind pedig a II. esetén az érintetteknek szóló tájékoztatást ki kell egészíteni

- az adatok megismerésére jogosult személyek körével,
- adatbiztonsági intézkedésekről szóló tájékoztatással.

4.1.3.3 Hozzáférés, helyesbítés, törlés, korlátozás, adathordozhatóság, és tiltakozás

A Társaságnak gondoskodnia kell arról, hogy az alábbiakban részletezett érintetti jogokat a 4.1.3.1-es, általános szabályokat leíró fejezetben foglaltaknak megfelelően biztosítsa.

Hozzáférési jog

Ha az érintett a Társasághoz eljuttatott kérelmében, hozzáférési jogával kíván élni, akkor a Társaság tájékoztatja arról, hogy személyes adatainak kezelése folyamatban van-e. Amennyiben folyamatban van, úgy a Társaság az érintett személyes adataihoz hozzáférést biztosít, valamint tájékoztatást nyújt

- az adatkezelés céljairól,
- a személyes adatok kategóriáiról,
- az adattovábbítás címzettjeiről,
- az adatok tárolásának időtartamáról,
- arról, hogy adott esetben kérheti a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen,
- Hatósághoz benyújtható panasz jogáról,
- ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információról,
- automatizált döntéshozatal tényéről, beleértve a profilalkotást is, valamint az ezekben az esetekben alkalmazott logikáról, és arról, hogy adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

Amennyiben a Társaság a személyes adatokat harmadik országba továbbítja, tájékoztatást nyújt a GDPR-ban foglalt egyéb garanciák meglétéről.

A Társaságnak biztosítania kell az érintett másolatigénylési jogának gyakorolhatóságát. A másolatot első alkalommal ingyenesen kell az érintett rendelkezésére bocsátani, további másolatokért adminisztratív költségeket lehet felszámítani. Adminisztratív költségként a kérés teljesítésére fordított munkaóra és a tényleges anyagköltség vehető figyelembe. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

Helyesbítéshez való jog

A Társaság az adatkezelést úgy alakítja ki, hogy az érintett kérelme esetén indokolatlan késedelem nélkül helyesbíteni tudja a rá vonatkozó, pontatlanul tárolt személyes adatokat, hiányos adatok esetén pedig az érintettől beszerezze a személyes adatokat, úgy, hogy a tájékoztatás és a hozzájárulás is megvalósuljon.

Törléshez való jog

Az érintett jogosult arra, hogy kérésére a Társaság indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, a Társaság pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha

- az adatkezelés célja megszűnt,
- az érintett visszavonja hozzájárulását, és más jogalap nincs az adatok kezelésére,
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
- a személyes adatokat jogellenesen kezelik,
- hozzájáruláson alapuló, közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelésére vonatkozik.

Amennyiben a Társaság által már nyilvánosságra hozott személyes adatokra vonatkozik az érintett megalapozott törlési igénye, akkor a technológia és a megvalósítás költségeit mérlegelve, a Társaságnak meg kell tennie az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat

kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

A törléshez való jogot korlátozhatja a véleménynyilvánítás szabadságához való jog, a jogi kötelezettség, a közérdek (közérdekű és a közérdekből nyilvános adatok kezelése), illetve ha az adatkezelés szükséges a jogi igények előterjesztéséhez, érvényesítéséhez, valamint védelméhez. A törléshez való jog korlátozhatósága esetenként mérlegelendő legalább az Adatvédelmi tisztviselő, valamint a Biztonsági Igazgatóság Információbiztonsági szakterület közreműködésének igénybevételével.

Korlátozás

A Társaságnak az érintett kérésére korlátoznia kell az adatkezelést, az alábbi esetekben:

- az érintett vitatja az adatok pontosságát, ekkor azok ellenőrzésének idejére kell korlátozni az adatkezelést,
- az adatkezelés jogellenes, és az érintett az adatok törlése helyett, azok felhasználásának korlátozását kéri,
- az adatkezelés célja megszűnt, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett tiltakozott az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Társaság jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A Társaságnak biztosítania kell, hogy a korlátozás alatt álló adatok csak az érintett hozzájárulásával, vagy mérlegeléssel alátámasztott jogos érdekből, vagy közérdekből legyenek kezelhetőek. Az elszámoltathatóság elvének való megfelelés érdekében, a korlátozás ilyen módon történő feloldásának dokumentálásáról, és jogszerűsége bizonyíthatóságáról a Társaságnak kell gondoskodnia.

A Társaságnak előzetesen tájékoztatnia kell az érintettet, a kérelmére történő korlátozás feloldásáról.

Adattovábbítás címzettjeinek értesítése

A Társaságnak minden olyan címzettet tájékoztatnia kell, a helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akinek az érintett adatait továbbították. Ez alól kivételt az jelent, ha a tájékoztatás lehetetlen, vagy aránytalanul nagy erőfeszítést igényel.

Adathordozhatóság

Amennyiben a Társaság az érintett személyes adatait automatizált módon kezeli, valamint az adatkezelés jogalapja az érintett GDPR 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja szerinti hozzájárulása- vagy a GDPR 6. cikk (1) bekezdésének b) pontja szerinti vele kötött szerződés, úgy az érintett által rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban kell a rendelkezésére bocsátani.

Az adathordozhatósághoz való jog gyakorlása, nem sértheti az adattörléshez való jogot leíró rendelkezésben foglaltakat, továbbá nem érintheti hátrányosan mások jogait és szabadságait.

Tiltakozáshoz való jog

Amennyiben a Társaság az érintett személyes adatait a GDPR 6. cikk (1) bekezdésének e) vagy f) pontja alapján kezeli, akkor az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is.

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben a Társaság a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Ha a személyes adatok kezelése közvetlen üzletszerzési cél érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

Amennyiben az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

Automatizált döntéshozatal egyedi ügyekben

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 említett 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 kivételekben említett döntések nem alapulhatnak a személyes adatoknak különleges kategóriáin 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.

4.1.4 Adatkezelő és adatfeldolgozó

4.1.4.1 Adatkezelő és közös adatkezelők

Főszabályként a Társaság felelős az általa kezelt személyes adatok védelméért, viszont ha az adatkezelés céljait és eszközeit egy másik adatkezelővel vagy adatkezelőkkel közösen határozzák meg, azok közös adatkezelőknek minősülnek.

Amennyiben a Társaság és egy vagy több további önálló jogalanyisággal rendelkező adatkezelő folytat közös adatkezelést, úgy írásbeli megállapodásban kell rendezni a felelősségi köröket, és ennek a megállapodásnak az adatkezelésre vonatkozó rendelkezéseit az érintettek rendelkezésére kell bocsátani. Jogszabályi rendelkezés is meghatározhatja az egyes adatkezelők kötelezettségeit egy közös adatkezeléssel kapcsolatosan. Az érintettek jogainak akadálytalan biztosítása érdekében, az érintettek jogaikat bármelyik adatkezelővel szemben gyakorolhatják.

4.1.4.2 Az adatfeldolgozó

A Társaság az egyes adatkezelési tevékenységeit kiszervezheti külső adatfeldolgozóknak, akik a Társaság megbízásából végzik az általa előre definiált adatkezelési műveleteket. Az adatfeldolgozó adatkezeléssel kapcsolatos döntéseket nem hozhat, kizárólag végrehajtja a Társasággal kötött megállapodásból fakadó kötelezettségeit. A Társaság felelőssége azt meghatározni, hogy az általa megbízott adatfeldolgozók megfelelő garanciákat nyújtsanak az adatvédelmi jogszabályoknak való megfeleléshez, és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtásához.

Az adatfeldolgozó által végzett adatkezelést olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint a Társaság kötelezettségeit és jogait meghatározó – szerződésnek kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben. A Társaságnak az adatfeldolgozói szerződésben elő kell írnia az adatfeldolgozót terhelő kötelezettségek körében, legalább az alábbiakat:

– a személyes adatokat kizárólag a Társaság írásbeli utasításai alapján kezeli, kivéve jogszabályban előírt egyedi esetekben,

- biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak,
- meghozza a megfelelő technikai és szervezési intézkedéseket, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja,
- a Társaság előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe,
- az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti a Társaságot abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében,
- segíti a Társaságot az adatkezelés biztonsága, az incidensmenedzsment, az adatvédelmi hatásvizsgálat és az előzetes konzultáció teljesítésében,
- az adatkezelési szolgáltatás nyújtásának befejezését követően a Társaság döntése alapján minden személyes adatot töröl vagy visszajuttat a Társaságnak, és törli a meglévő másolatokat, kivéve, ha jogszabály másként rendelkezik,
- a Társaság rendelkezésére bocsát minden olyan információt, amely az adatfeldolgozó igénybevételével kapcsolatos kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti a Társaság által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is. Ezen információknak a Társaság rendelkezésére bocsátásával kapcsolatosan az adatfeldolgozónak haladéktalanul tájékoztatnia kell a Társaságot, ha úgy véli, hogy annak valamely utasítása adatvédelmi jogszabályt sért.

A Társaságnak az adatfeldolgozóval kötött adatfeldolgozói szerződésben ki kell térnie továbbá arra, hogy amennyiben az adatfeldolgozó, további adatfeldolgozót vesz igénybe, úgy ugyanazokat az adatvédelmi kötelezettségeket kell meghatározni a további adatfeldolgozóra, mint amelyeket az adatkezelési szerződésben meghatározott a Társaság az adatfeldolgozó számára.

4.2 Általános feladatok, felelősségek és hatáskörök

Vezérigazgató

Gondoskodnia kell a Társaság adatvédelmi stratégiájának jóváhagyásáról.

A Biztonsági Igazgató tájékoztatása alapján, az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetését el kell rendelnie.

Adatkezelő szervezeti egység vezetője

Gondoskodnia kell az adatvédelmi munkacsoport tagjainak kijelöléséről.

Az adatvédelmi munkacsoporttól kapott – az előírásoktól eltérő adatkezelési gyakorlatra vonatkozó – értesítés esetén gondoskodnia kell a szabályszerű állapot helyreállításáról.

Amennyiben a Társaságon belüli Adatkezelő szervezeti egységek együttesen folytatnak közös adatkezelést, akkor az adatkezeléssel járó szakmai folyamatot leíró utasításban kell rendezniük az adatkezelés kapcsán felmerült kötelezettségeiket, különös tekintettel az érintettek tájékoztatására és jogaik gyakorlásának biztosítására.

Az adatkezelő szervezeti egység vezetője az adatvédelmi tisztviselő szakmai javaslata alapján dönt az adatvédelmi tisztviselő ellenőrzése során tett megállapítások és javaslatok foganatosítása tekintetében. Ha az adatkezelő szervezeti egység vezetője nem veszi figyelembe a szakmai javaslatot, akkor írásban köteles megindokolni a szakmai javaslatban megfogalmazottak figyelmen kívül hagyását és azt, hogy a döntése során milyen módon juttatja érvényre az adatvédelmi elveket és e Szabályzat előírásait.

Biztonsági Igazgató

Tájékoztatnia kell a Vezérigazgatót az adatkezelésre irányuló ellenőrzés során feltárt hiányosságokról vagy jogszabálysértő körülményekről.

Munkáltatói jogkörgyakorló minőségében felügyelnie kell az Adatvédelmi tisztviselő munkavégzését.

Éves adatbiztonsági ellenőrzési tervet kell elfogadnia.

Adatbiztonsági vizsgálatot rendelhet el.

Feladatai ellátása során jogosult teljes mértékben betekinteni a Társaságnál végzett

összes adatkezelés és adatfeldolgozás dokumentumaiba, és jogosult teljes körű tájékoztatást kapni a vizsgált adatkezelésekről. Minden olyan adatkezelést megismerhet, amely személyes adatokkal összefügghet, és minden helyiségbe beléphet, ahol adatkezelés folyik.

Adatvédelmi tisztviselő

Írásbeli tájékoztatást és szakmai tanácsot, állásfoglalást kell adnia az adatkezelő és az adatkezelést végző alkalmazottak részére.

Ki kell alakítania az adatvédelmi munkacsoportot, munkájukhoz szakmai támogatást kell nyújtania, folyamatos képzésüket biztosítania kell a 71/2018. (XII. 20. MÁV-START Ért. 42.) sz. vezérigazgatói utasítás a MÁV-START Zrt. képzési tevékenységéről szóló utasításban foglaltak figyelembe vételével.

Az adatvédelmi tisztviselő ellenőrzi a GDPR-nek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az Adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is.

Az adatvédelmi tisztviselő értesíti az ellenőrizni kívánt szervezeti egység vezetőjét és az adott területhez tartozó szűkített adatvédelmi munkacsoport tagot. az auditról/ellenőrzésről. Az ellenőrzés során tett észrevételeket és javaslatokat az adatvédelmi tisztviselő írásban megküldi az adott szervezeti egység vezetőjének.

Az adatkezelő szervezeti egység vezetője az adatvédelmi tisztviselő szakmai javaslata alapján dönt az ellenőrzés során tett megállapítások és javaslatok foganatosítása tekintetében. Ha az adatkezelő szervezeti egység vezetője nem veszi figyelembe a szakmai javaslatot, akkor írásban köteles megindokolni a szakmai javaslatban megfogalmazottak figyelmen kívül hagyását és azt, hogy a döntése során milyen módon juttatja érvényre az adatvédelmi elveket és e Szabályzat előírásait. A szervezeti egység vezető szakmai javaslat ellenében meghozott döntése nem lehet e Szabályzatba foglaltakkal ellentétes. Amennyiben a szervezeti egység vezetője az adatvédelmi tisztviselő szakmai javaslata ellenében dönt, úgy az írásbeli indoklását az adatvédelmi tisztviselő köteles felülvizsgálni. Amennyiben az adatvédelmi tisztviselő úgy ítéli meg, hogy a döntéshozó döntése nem felel meg az adatvédelmi elveknek és e Szabályzat előírásainak, erről feljegyzést készít a biztonsági igazgató részére.

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

Információbiztonsági szakterület

Éves ellenőrzési tervet kell készítenie, továbbá a Társaság rendszereiben és számítógépes alkalmazásaiban ellenőriznie kell az adatbiztonsági követelmények megvalósulását.

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

Adatvédelmi munkacsoport

Az adatvédelmi munkacsoport a Társaság adatkezelő szervezeti egységeinek munkatársaiból áll. A munkacsoport tagok feladata az adatvédelmi megfelelés elősegítése, illetve kapcsolattartás az őt delegáló szervezeti egység és az adatvédelmi tisztviselő között. Támogatnia kell az Adatkezelő szervezeti egységét a jelen szabályzat előírásainak végrehajtásában. Figyelemmel kell kísérnie a szervezeti egységénél folytatott adatkezeléseket. Az előírásoktól eltérő adatkezelési gyakorlat észlelése esetén értesítenie kell az adatkezelést végző szervezeti egység vezetőjét.

A munkacsoporttagokat az adatkezelő delegálja, azon munkavállalói közül, akik ismerik a szervezet által végzett munkafolyamatokat.

Az adatkezelők által delegált munkacsoporttagok száma függ az adott szervezeti egység adatkezelésinek számától, illetve annak összetettségétől. Szükség szerint az adatvédelmi tisztviselő ajánlást tesz további munkacsoport tag delegálására.

Az adatvédelmi tisztviselő adatvédelmi kérdésekkel kapcsolatban a munkacsoport tagok rendelkezésére áll, tájékoztatást- és szakmai támogatást nyújt részükre.

A munkacsoporttagok folyamatos belső képzéséről az adatvédelmi tisztviselő-, külső képzéséről, adott esetben adatvédelmi konferenciákon történő részvételéről az adatkezelő gondoskodik.

Az adatvédelmi munkacsoport részére az adatvédelmi tisztviselő évente legalább egyszer értekezletet tart.

Szűkített adatvédelmi munkacsoport

Az adatvédelmi munkacsoport tagjai közül az adatkezelő szervezeti egység vezetője delegál egy főt a szűkített adatvédelmi munkacsoportba, mely munkacsoport tagjai évente legalább kétszer, de eseti jelleggel akár többször is részt vesznek az adatvédelmi tisztviselő által vezetett értekezleten. Ezen munkavállalók folyamatos képzésben részesülnek, közvetlenül segítik az adatvédelmi tisztviselő munkáját a szervezeti egységükkel kapcsolatos adatkezelések tekintetében, így különösen:

- a szervezeti egységnél bevezetésre kerülő új adatkezelési folyamat tervezési szakaszába bevonja az adatvédelmi tisztviselőt,
- az adatvédelmi tisztviselőnek folyamatos változásjelentési kötelezettséggel tartozik,
- naprakészen tartja az adatkezelési nyilvántartást, amelyben ha változás áll be, azt azonnal közli az adatvédelmi tisztviselővel,
- adatvédelmi incidens esetén részt vesz az incidens kivizsgálásában, a szükséges dokumentumok létrehozásában, kitöltésében,
- a NAIH megkeresése esetén részt vesz a tények kiderítésében, az információk összegyűjtésében és a választervezet elkészítésében.

Az adatvédelmi munkacsoport és a szűkített adatvédelmi munkacsoport tagjai kötelesek minden, az adott szervezeti egységet érintő, adatvédelmi tárgyú megbeszélésen részt venni.

Adatvédelmi szakértői csoport:

Az adatvédelmi tisztviselő közvetlen irányítása alatt álló szakértői csoport, ami segíti a szervezeti egységek és az adatvédelmi tisztviselő munkáját a szükséges dokumentumok, folyamatok előkészítésével. Folyamatos oktatásban részesülnek akár az adatvédelmi tisztviselő, akár külső képzés által. Feladatuk a folyamatok adatvédelmi szempontú átvizsgálásának segítése. Az adatvédelmi incidensről jogszabály által előírt információk beszerzése, az érintett szervezeti egység választervezetének felülvizsgálata. Részvétel az adatvédelmi tárgyú megbeszéléseken. Részvétel az utasítások adatvédelmi szempontú átvilágításában.

Az adatvédelmi szabályok beépítése az adatkezelő szervezeti egység munkavállalóival az egyes utasításokba/szabályzatokba. Segít az adatkezelési tájékoztatók megírásában az adott szervezeti egységeknek és adatvédelmi munkacsoport tagjainak. Részt vesz a NAIH megkeresések megválaszolásának előkészítésében, segíti az érintett szervezeti egységet. Javaslatot tesz az adatvédelmi tisztviselőnek az ellenőrizendő adatkezelésekről. Az adatvédelmi tisztviselőhöz érkező adatvédelmi állásfoglalások előkészítése. Folyamatos oktatás, újfelvételesek oktatása.

Az adatvédelmi tisztviselő bármely adatvédelmi tárgyú megbeszélésre és feladat ellátására delegálhatja az adatvédelmi szakértői csoport bármely tagját, kivéve azon feladatokat, melyeket a jogszabály kifejezetten az adatvédelmi tisztviselő feladatkörébe vont.

Az adatvédelmi csoport tagja megfelelő szakmai tudással és tapasztalattal bíró, jó kommunikációs, valamint jó problémamegoldó készséggel és angol középfokú nyelvismerettel rendelkező személy.

4.3 Feladatok és felelősségek az adatkezelés megkezdése előtt

Az utasítás jelen szakasza 4.3-as ponttól a 4.5-ös pontig bezáróan az adatkezeléssel járó szakmai folyamatért felelős, adatkezelő szervezeti egység és egyéb résztvevők feladat és felelősségét határozza meg az adatkezelés egyes szakaszaiban. Az előbbiekben jelzett szakaszokban helyenként visszautalás történik az általános leírást tartalmazó 4.1-es pontra, ahol bár adatkezelőként a Társaság került

megjelölésre, a feladatok és felelősségek továbbra is az adott szakmai folyamatért felelős Adatkezelő szervezeti egységet terhelik.

4.3.1 Az Adatkezelő szervezeti egység feladata

Az adott szervezeti egységnél zajló egyes adatkezeléssel járó szakmai folyamatok adatvédelmi megfelelősége, az ilyen folyamatok kialakítása, az elkészült folyamatnak és folyamatábrának Adatvédelmi tisztviselővel történő dokumentált megismertetése az Adatkezelő szervezeti egység vezetőjének felelősségi körébe tartozik.

Az Adatkezelő szervezeti egységnek az adatkezeléssel járó folyamat megtervezésének kezdetén be kell vonnia az Adatvédelmi tisztviselőt, hogy szakmai segítséget nyújtson a megfeleléshez.

Az Adatkezelő szervezeti egységnek az Adatvédelmi tisztviselő közreműködésével úgy kell kialakítania az adatkezeléssel járó tevékenységét, hogy az megfeleljen a hatályos jogszabályoknak, dokumentált legyen, biztosítsa az érintettek jogainak gyakorlását, és szavatolja a személyes adatok biztonságát.

4.3.1.1 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 folytatnia. Az adatvédelmi hatásvizsgálat lefolytatásában az Adatkezelő szervezeti egységnek az Adatvédelmi tisztviselő szakmai segítségét kell kérnie.

Az adatvédelmi hatásvizsgálat elvégzése minden esetben kötelező különösen, ha:

- 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 a Hatóság által közzétett, kötelező eseteket tartalmazó listán.

Amennyiben az adatkezeléssel járó tevékenység nem esik a fent említett kategóriákba, a hatásvizsgálat szükségességének eldöntéséhez az alábbi kockázati tényezők meglétét kell mérlegelni:

- Értékelés vagy pontozás, ideértve a profilalkotást és az előrejelzést is, különösen az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján.
- 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.
- Módszeres megfigyelés: érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztüli adatgyűjtés vagy a nyilvános helyek nagymértékű, módszeres megfigyelése.
- Különleges adatok vagy fokozottan személyes jellegű adatok kezelése.
- Nagy számban kezelt adatok:
  - = 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.

- 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.
- Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok
  = gyermekek
  = munkavállalók
  = lakosság különleges védelmet igénylő rétegei vagy
  = minden olyan esetben, amikor az érintett és az adatkezelő közötti kapcsolatban egyenlőtlen helyzet alakul ki.
- Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: például az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében.
- 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.

Amennyiben az Adatkezelő szervezeti egység, a fent említett körülmények vizsgálata alapján, és az Adatvédelmi tisztviselő állásfoglalása ellenére a hatásvizsgálat lefolytatását mellőzi, úgy dokumentáltan alá kell támasztania az adatvédelmi hatásvizsgálat mellőzésének okait.

Az adatvédelmi hatásvizsgálat elvégzése nem kötelező ha:

- ha az adatkezelés valószínűsíthetően nem jár magas kockázattal a természetes személyek jogaira és szabadságaira nézve,
- ha 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,
- ha az adatkezelési műveleteket a Hatóság 2018. május előtt már ellenőrizte és az adatkezelés feltételei azóta nem változtak meg,
- ha az adatkezelés jogi kötelezettség teljesítésén- vagy közérdeken-, vagy közhatalmi jogosítvány gyakorlásán alapszik; és jogszabály szabályozza az adott adatkezelési műveletet; és ezen jogszabály alapján végzett adatkezelésre már készült adatvédelmi hatásvizsgálat; feltéve, hogy a jogszabályban nincs kifejezetten kimondva, hogy minden esetben hatásvizsgálatot kell végezni,
- ha az adatkezelés szerepel a Hatóság által összeállított, a nem kötelező adatkezelési műveletek jegyzékében, amelyekre tekintettel nem kötelező hatásvizsgálatot készíteni.

Az adatvédelmi hatásvizsgálatot rendszeres időközönként felül kell vizsgálnia az Adatkezelő szervezeti egységnek. A felülvizsgálatot legalább kétévente el kell végezni. A felülvizsgálatot haladéktalanul le kell folytatni, amennyiben az adatkezelés lényeges körülményei:

- a hatókör,
- a cél,
- a gyűjtött személyes adatok köre,
- az adatkezelők vagy címzettek kiléte,
- az adatmegőrzési időszak,
- a technikai és szervezési intézkedések,
- az alkalmazott technológia

változnak.

Érintettek véleményének kikérése

Az Adatkezelő szervezeti egységnek ki kell kérnie az érintettek vagy képviselőik véleményét a tervezett adatkezelésről. Mellőzhető az érintettek véleményének kikérése, ha az által a Társaság üzleti tervének titkossága sérülne, illetve aránytalan vagy kivitelezhetetlen lenne ez az intézkedés. Amennyiben az Adatkezelő szervezeti egység úgy dönt, hogy nem kéri ki az érintettek véleményét, akkor nemleges döntését dokumentumokkal kell alátámasztania.

Hatásvizsgálat lefolytatása, és az előzetes konzultáció

Az Adatkezelő szervezeti egységnek az 1. számú melléklet alapján kell elvégeznie az adatvédelmi hatásvizsgálatot. Amennyiben a Hatóság honlapjáról letölthető adatvédelmi hatásvizsgálat szoftver rendelkezésre áll az Adatkezelő szervezeti egység részére, úgy az adatvédelmi hatásvizsgálatot annak segítségével kell elvégezni.

Amennyiben a hatásvizsgálat eredménye alapján, a kockázatmérséklő intézkedések ellenére, az adatkezelés továbbra is valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira, úgy az Adatkezelő szervezeti egység az Adatvédelmi tisztviselő szakmai támogatása mellett előzetes konzultációt kell, hogy kezdeményezzen a Hatósággal.

Az előzetes konzultáció során az Adatkezelő szervezeti egységnek tájékoztatást kell adnia a Hatóságnak:

- az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről, különösen vállalkozáscsoporton belüli adatkezelés esetén;
- 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 a Hatóság az előzetes konzultáció iránti megkeresésre a kézhezvételétől számított nyolc héten belül ad írásban tanácsot, illetve ez a 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.

4.3.1.2 Jogalap

Az Adatkezelő szervezeti egységnek az adatkezelés megkezdését megelőzően meg kell határoznia az adatkezelés jogalapját figyelemmel a 4.1.2. pontban foglaltakra.

4.3.1.3 Érdekmérlegelési teszt

Amennyiben a jogalap meghatározása a GDPR 6. cikk (1) bekezdés f) pontja, azaz a Társaság jogos érdeke, úgy az Adatkezelő szervezeti egységnek érdekmérlegelési tesztet kell végeznie (2. sz. melléklet szerint).

Érdekmérlegelési teszt elkészítésének folyamata:

1. lépés: a Társaság a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.

2. lépés: a Társaság a jogos érdekét a lehető legpontosabban meghatározza.

3. lépés: a Társaság meghatározza, hogy mi az adatkezelés célja, milyen személyes adatok, milyen időtartammal történő adatkezelését igényli a jogos érdek.

4. lépés: a Társaság meghatározza, hogy az érintetteknek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (pl. azok a szempontok, amelyeket az érintettek érvként felhozhatnának az adatkezeléssel szemben).

5. lépés: a Társaság elvégzi jogos érdekeinek és az érintettek érdekeinek, alapjogainak súlyozását és ez alapján megállapítja, hogy a személyes adat kezelhető-e. A Társaság meghatározza, hogy miért korlátozza arányosan a Társaság jogos érdeke – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott érdekelti jogokat, várakozásokat.

6. lépés: a Társaság meghatározza, mely garanciák biztosíthatják az adatkezelés szükségességét-arányosságát (természetesen más garanciális intézkedések is alkalmazhatók).

7. lépés: Érdekmérlegelés eredménye és annak dokumentálása.

4.3.1.4. Adatbiztonság

Az Adatkezelő szervezeti egység felelőssége, hogy az adatkezelés megtervezése folyamán

- 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 hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Ezen intézkedések, többek között

- 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.

Miután az adatkezelés megtervezésének folyamata abba a szakaszba ért, hogy a jogszerűség-, tisztességes eljárás- és átláthatóság-, adattakarékosság-, pontosság-, korlátozott tárolhatóság-, elvének érvényesülése biztosított, – tehát az adatkezelő az Adatvédelmi tisztviselő bevonásával megtervezte az adatkezeléssel járó tevékenységét és meghatározta a kezelni kívánt adatok körét – az integritás- és bizalmas jelleg- elvének való megfelelés elősegítése érdekében az adatkezelő bevonja a Biztonsági Igazgatóság Információvédelemi szakterületét.

Technikai elvárások a tervezés során:

- A személyes adatokat tároló számítógépes adathordozóját teljes kapacitásában titkosítani kell.
- Külön védelmi intézkedéseket kell tenni, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.
- A szerver számítógépek és a munkaállomások között személyes adatokat védetten (titkosítva) kell továbbítani.
- A Társaság alkalmazottainak és ügyfeleinek személyes adatait tartalmazó adatbázisokat a Társaság Informatikai Biztonsági Szabályzatában (a továbbiakban: IBSZ) definiált ún. **bizalmasság és sértetlenség szerinti** „fokozott” **biztonsági osztálynak megfelelő** védelemben kell részesíteni.
- A rendszerekben a felhasználói jogosultságok korlátozásával biztosítani kell, hogy a hozzáférésre jogosultak kizárólag a munkájukhoz feltétlenül szükséges személyes adatokat ismerhessék csak meg. A rendszereket a Társaság IBSZ-ében foglalt előírások szerint kell kifejleszteni, az ott előírt biztonsági dokumentumok elkészültét követően szabad használatba venni és üzemeltetni.
- Személyes adatot tartalmazó valamennyi dokumentumot ”Nem nyilvános!” kezelési jelzéssel kell ellátni. A jelzést a dokumentum (pl.: munkaszerződés, fizetési besorolás, a személyes adatokat tartalmazó adatbázis felhasználásával készített Excel-táblázat, Utasleadási lap, kedvezményes utazásra jogosító kártya igénylőlapja) minden egyes lapjának fejrészében a készítőnek fel kell tüntetnie. E minősítési jelzés mellett az ilyen dokumentumot iktatási számmal is el kell látni, kivéve, ha azon más, a dokumentum egyedi azonosítására alkalmas jelzés található.
- Ha a személyes adat számítógépes képernyőn kerül megjelenítésre, akkor a képernyő felső részén meg kell jeleníteni a ”Nem nyilvános!” kezelési jelzést. A monitort úgy kell elhelyezni, hogy a többszemélyes irodában dolgozók, és az irodába belépő más személyek illetéktelenül ne ismerhessék meg a képernyőn megjelenő személyes adatokat.

– Személyes adat másolása az elektronikus adathordozóra kizárólag titkosított módon történhet. A „Nem nyilvános” jelzéssel ellátott dokumentumokat, és a személyes adatokat tartalmazó adathordozókat biztonsági zárral ellátott fa szekrényben, vagy lemezszekrényben kell tárolni. A rontott és a munkapéldányokat megsemmisítésükig ugyanezen szabályok szerint kell tárolni.

4.3.1.5 Érintetti jogok, és az érintett tájékoztatása

Érintetti jogok

Az Adatkezelő szervezeti egységnek úgy kell kialakítania az adatkezeléssel járó szakmai folyamatait, hogy a 4.1.3. pontban foglalt érintetti jogok gyakorolhatóságát biztosítani tudja.

Adatvédelmi tájékoztató elkészítése

Az Adatkezelő szervezeti egységnek jelen utasítás 4.3.2. pontja, valamint 4. sz. melléklete alapján kell elkészítenie az adatkezelési tájékoztatót.

4.3.1.6 Adatkezelés nyilvántartása

Az Adatkezelő szervezeti egység az adatkezelésről nyilvántartást vezet. Az adatkezelést bejelenti az Adatvédelmi tisztviselő részére, aki vezeti a Társasági szintű Belső adatvédelmi nyilvántartást.

4.3.1.6.1 Az adatkezelő szervezeti egység feladata

Az Adatkezelő szervezeti egység az adatkezeléssel járó tevékenységeiről a 3. sz. mellékletben előírtak szerint kitölti a Belső adatvédelmi nyilvántartásba bejelentő lapot és a Társaság Irat és Dokumentumkezelő Rendszerében nyilvántartásba veszi. Az Adatkezelő szervezeti egységnek az adatkezelés megkezdése előtt a 3. sz. mellékletet meg kell küldenie az Adatvédelmi tisztviselő részére, aki felveszi a Belső adatvédelmi nyilvántartásba.

4.3.1.6.2 Az Adatvédelmi tisztviselő feladata

Az adatkezeléssel járó szakmai folyamatok megtervezésében történő bevonását követően, dokumentált szakmai tanácsot kell adnia az Adatkezelő szervezeti egység részére.

Az Adatvédelmi tisztviselőnek szakmai tanácsot kell adnia az adatvédelmi hatásvizsgálat lefolytatásának szükségességére, illetve az Adatkezelő szervezeti egység által előkészített hatásvizsgálatot értékelnie kell, valamint az elkészített hatásvizsgálatot véleményeznie kell.

Amennyiben a hatásvizsgálat eredménye alapján, a kockázatmérséklő intézkedések ellenére, az adatkezelés továbbra is valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira, úgy az Adatkezelő szervezeti egység kezdeményezésére indított előzetes konzultációhoz szakmai segítséget kell nyújtania.

Az érdekmérlegelési tesztbe történő bevonása esetén, szakmai tanácsot kell adnia az Adatkezelő szervezeti egység részére.

A szakmai tanácsadásnak ki kell terjednie az érintetti jogok biztosításának rendjére, illetve az érintett előzetes tájékoztatására, azaz az adatvédelmi tájékoztatók összeállítására is.

Az Adatvédelmi tisztviselőnek egy Társasági szintű összesített Belső adatvédelmi nyilvántartást kell vezetnie. A Belső adatvédelmi nyilvántartás adattartalmát az Adatkezelő szervezeti egységektől megkapott Belső adatvédelmi nyilvántartásba bejelentő lapok (3. sz. melléklet) képzik. A belső adatvédelmi nyilvántartásban az egyes adatkezeléseket egyedi azonosítóval kell ellátni, amelyet az Adatvédelmi tisztviselőnek kell vezetnie.

Az Adatvédelmi tisztviselőnek az általa végzett tevékenységéről havi lebontásban nyilvántartást kell vezetnie, amelyet a tárgyhónapot követő hónap 10. napjáig kell az Irat és Dokumentumkezelő Rendszeren keresztül a munkáltatói jogkörgyakorló részére eljuttatnia. A nyilvántartást, jelen utasítás 6. sz. melléklete szerint kell elkészítenie.

A nyilvántartás tartalmi elemei

– *Sorszám*
– *Dátum:* A tevékenység időpontja / intervalluma.
– *Tevékenység típusa*: A tevékenység rövid összefoglalása. (pl.: érintettek tájékoztatása, szakmai állásfoglalás, adatvédelmi incidens kivizsgálása, Hatóság tájékoztatása, közreműködés hatásvizsgálatban)

- *Tevékenység leírása*: Annak részletes kifejtése, hogy
  - = a tevékenységet kinek a részére végezte (pl.: Hatóság megnevezése, Adatkezelő szervezeti egység megnevezése, adatkezeléssel érintettek köre)
  - = milyen ügyben, adatkezeléssel kapcsolatos a tevékenység
  - = konkrét tevékenység leírása
  - = a tevékenység eredménye
  - = amennyiben van, akkor a tevékenység végrehajtásának határideje
- *Keletkezett dokumentumok/iktatószámok*

Statisztikai adatok:

- Előző hónap végén a Belső adatvédelmi nyilvántartásban szereplő adatkezelések összesített száma:
- A hónapban a Belső adatvédelmi nyilvántartásba újonnan regisztrált adatkezelések száma:
- Előző hónap végén a tárgyévben történt adatvédelmi incidensek összesített száma:
- A hónapban történt adatvédelmi incidensek száma:
- Folyamatban lévő Hatósági adatvédelmi eljárások száma:
- Folyamatban lévő Hatósági adatvédelmi vizsgálatok száma:

4.3.2 A Biztonsági igazgatóság információbiztonsági szakterület feladata

Az Információvédelemi szakterület támogatást nyújt az adatkezelő részére az adatkezelési tevékenység adatbiztonsági követelményeinek kialakításában. A kezelt adatok biztonsága érdekében be kell tartani a Társaság mindenkori hatályos Informatikai Biztonsági Szabályzatának-, valamint Iratkezelési Szabályzatának előírásait.

Az adatvédelmi hatásvizsgálat lefolytatása során a felmerülő adatbiztonsági kockázatok feltárása, mérséklése érdekében az Adatkezelő szervezeti egység megkeresése esetén szakmai segítséget kell, hogy nyújtson.

Az adatvédelmi tájékoztató elkészítése során az Adatkezelő szervezeti egység megkeresése esetén a tájékoztató „Adatbiztonsági intézkedésekről szóló tájékoztatás” rész kitöltéséhez szakmai segítséget nyújt.

4.4 Feladatok és felelősségek a személyes adatok kezelése során

A személyes adatok kezelése során a kialakított nyilvántartásokat naprakészen kell tartani, a bekövetkezett incidenseket kezelni kell, a hatásvizsgálatokat felül kell vizsgálni, a személyes adatok kezelése során az érintettek részére jogaik gyakorlását lehetővé kell tenni.

A Társaság minden munkavállalója és a Társasággal szerződésben álló szervezetek minden munkatársa köteles az általa megismert, vagy számára bejelentett adatvédelmi incidenst – a lehető leghamarabb, de legkésőbb annak tudomására jutásától számított 4 órán belül – jelenteni az Adatvédelmi tisztviselőnek az adatvedelem@mav-start.hu e-mail elérhetőségen.

4.4.1 Az Adatkezelő szervezeti egység feladata

4.4.1.1 Adatkezeléssel járó szakmai folyamat módosítása, időszakos felülvizsgálata

Amennyiben az személyes adatkezeléssel járó szakmai folyamatban olyan lényeges változás következik be, amely a személyes adatok kezelésére is hatással van, úgy az új szakmai folyamat tervezésénél ismét figyelembe kell venni jelen utasítás 4.3. pontjában foglaltakat. Ha az adatkezeléssel járó szakmai folyamatban nem következik be változás, akkor is két évente felül kell vizsgálni az adatkezeléssel járó szakmai folyamatokat leíró utasításokat. Továbbá, adatvédelmi incidens bekövetkezése-, valamint a személyes adatkezelést érintő jogszabályi változás esetén is felül kell vizsgálni az adatkezeléssel járó szakmai folyamatot, illetve az azt leíró utasításokat.

4.4.1.2 Adatvédelmi hatásvizsgálat felülvizsgálata

Az adatvédelmi hatásvizsgálatot felül kell vizsgálni és újra kell értékelni, valahányszor csak olyan változás következik be az adatkezelésben vagy a rá ható külső körülményekben, amely magas kockázati szintet eredményez.

Ezen túlmenően az Adatkezelő szervezeti egységnek kétévente felül kell vizsgálnia és újra kell értékelnie a hatásvizsgálatot, függetlenül attól, hogy az adatkezelés körülményeiben történt-e változás, és annak eredményeként az adatvédelmi hatásvizsgálatot aktualizálni kell.

Az Adatkezelő szervezeti egységnek a hatásvizsgálat felülvizsgálata és újraértékelése során a 4.3.1.1. pont vonatkozó rendelkezéseire kell figyelemmel lennie.

4.4.1.3 Érintetti jogok biztosításával összefüggő feladatok

Az adatkezelési tájékoztatókon szerepeltetett elérhetőségeken keresztül, az érintettektől érkező megkereséseket az Adatkezelő szervezeti egységnek kell kezelnie, a tervezés folyamán a 4.3.1.5-ös pont szerint kialakított belső folyamat szerint. Az Adatkezelő szervezeti egység az Adatvédelmi tisztviselő szakmai segítségét kérheti a megkeresések teljesítése érdekében.

Amennyiben az érintett vitatja az Adatkezelő szervezeti egység eljárásának jogszerűségét, úgy az Adatkezelő szervezeti egységnek felül kell vizsgálnia a vitatott eljárását a jelen utasítás 4.3. pont szerint. Amennyiben nem ért egyet az érintett az Adatkezelő szervezeti egység az érintett észrevételével, úgy az Adatvédelmi tisztviselőhöz kell, hogy irányítsa.

Az érintett részéről érkezett megkereséseket az Adatkezelő szervezeti egységnek a 4.3. pontban meghatározott határidők betartása mellett kell teljesítenie.

4.4.1.4 Incidenskezelés

Az Adatvédelmi tisztviselő szakmai támogatása mellett az Adatkezelő szervezeti egységnek össze kell gyűjtenie mindazokat az információkat, ami alapján az Adatvédelmi tisztviselő ki tudja tölteni az 5. sz. mellékletet, az Adatvédelmi Incidens nyilvántartást.

Az Adatvédelmi tisztviselő számára megküldött bejelentésnek tartalmaznia kell legalább:

- az incidensről való tudomásszerzés időpontját,
- az incidens jellegét, tárgyát, rövid leírását,
- az incidenssel kapcsolatban rendelkezésre álló valamennyi információt.

Amennyiben az adatvédelmi incidens adatbiztonsági vagy informatikai szakmai kérdést érint, úgy az Adatkezelő szervezeti egység a Biztonsági igazgatóság információbiztonsági szakterületének vagy az Informatika szervezet szakmai segítségét kérheti.

Az így összegyűjtött információk birtokában az Adatvédelmi tisztviselő szakmai támogatása mellett, az Adatkezelő szervezeti egység el kell, hogy végezze az incidens hatásának mérlegelését, hogy az valószínűsíthetően kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve.

Amennyiben a mérlegelés eredményeként az incidens kockázattal jár a természetes személyek jogaira és szabadságára nézve, az Adatkezelő szervezeti egység az Adatvédelmi tisztviselőn keresztül be kell, hogy jelentse a Hatóság részére. Az Adatkezelő szervezeti egységnek ezt úgy kell megtennie, hogy az Adatvédelmi tisztviselőnek lehetőség szerint az észlelésétől számított 72 órán belül be kell jelentenie az incidenst a Hatóság részére. Ha a Hatóságnak történő bejelentés alkalmával, nem lehetséges az információkat egyidejűleg közölni, akkor azok további indokolatlan késedelem nélkül, később részletekben kell közölni, amelyhez mellékelni kell a késedelem igazolására szolgáló indokokat is.

Amennyiben a mérlegelés eredményeként az incidens magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, az Adatvédelmi tisztviselő szakmai támogatása mellett, a hatósági bejelentésen túl, köteles az incidenssel érintetteket tájékoztatni az alábbiakról:

- az Adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetősége,
- az adatvédelmi incidensből eredő, valószínűsíthető következmények,
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Nem kell az érintetteket tájékoztatni:

- ha a Társaság olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét;

– ha az adatvédelmi incidens bekövetkezését követően a Társaság olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg;
– ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

4.4.2 Az Adatvédelmi tisztviselő feladatai

Az Adatvédelmi tisztviselőnek az Adatkezelő szervezeti egység kérésére szakmai támogatást kell nyújtania az adatkezeléssel járó szakmai folyamatok felülvizsgálatához, adatvédelmi hatásvizsgálat felülvizsgálatához, és az érintetti jogokkal kapcsolatos igények teljesítéséhez.

Az Adatvédelmi tisztviselőnek kell irányítania a Társaság adatkezelési tevékenysége során bekövetkezett adatvédelmi incidensek kivizsgálását, ellenőriznie kell az adatkezelő által végzett incidenskezelést.

Az Adatvédelmi tisztviselőnek a hozzá megküldött adatvédelmi incidensekről nyilvántartást kell vezetnie az 5. sz. melléklet szerinti adattartalommal.

Az Adatvédelmi tisztviselőnek szakmai támogatást kell nyújtania az adatvédelmi incidensek kivizsgálásában, különös tekintettel az incidens hatásának mérlegelésében. Amennyiben a mérlegelés eredményeként az incidens kockázattal jár a természetes személyek jogaira és szabadságára nézve, az Adatkezelő szervezeti egység által összegyűjtött információkat be kell jelentenie a Hatóságnak az erre a célra kialakított online felületen keresztül.
(https://dbn-online.naih.hu/public/login)

Az incidenst lehetőség szerint az észlelésétől számított 72 órán belül kell a Hatóságnak jelenteni. Ha a Hatóságnak történő bejelentés alkalmával, nem lehetséges az információkat egyidejűleg közölni, akkor azok további indokolatlan késedelem nélkül, később részletekben kell közölni, amelyhez mellékelni kell a késedelem igazolására szolgáló indokokat is. Amennyiben a mérlegelés eredményeként az incidens magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, az Adatvédelmi tisztviselő köteles szakmai támogatást nyújtani az Adatkezelő szervezeti egység részére az incidenssel érintettek tájékoztatásában.

Az Adatvédelmi tisztviselőnek kapcsolattartóként kell szolgálnia a Hatóság felé:
– be kell jelentkeznie az Adatvédelmi tisztviselők nyilvántartásába,
– szakmai kérdésekben konzultációt kell folytatnia a Hatósággal, különös tekintettel a hatásvizsgálatra,
– a Hatóság által indított vizsgálatokban, eljárásokban közre kell működnie,
– Az Adatvédelmi tisztviselőnek a Társaság adatkezeléseinek valamennyi érintettje számára elérhetőnek kell lennie a Társaság honlapján-, illetve az adatkezelési tájékoztatókban feltüntetett elérhetőségein keresztül.

Amennyiben az érintettektől érkező megkeresések kezelése érdekében az Adatkezelő szervezeti egység az Adatvédelmi tisztviselő szakmai segítését kéri, úgy az Adatvédelmi tisztviselő köteles a szakmai segítséget megadni.

Ha az érintett vitatta az Adatkezelő szervezeti egység eljárásának jogszerűségét, úgy az Adatvédelmi tisztviselőnek vizsgálatot kell folytatnia. Amennyiben az Adatvédelmi tisztviselő vizsgálata eredményeként beigazolódik, hogy az adatkezelő nem megfelelően járt el, úgy fel kell, hogy szólítsa az Adatkezelő szervezeti egységet a jogszerű állapot visszaállítására.

4.4.3 A Biztonsági igazgatóság információbiztonsági szakterületének feladata

Az Adatkezelő szervezeti egység kérésére, adatbiztonsági kérdésekben szakmai támogatást kell nyújtania az adatkezeléssel járó szakmai folyamatok-, és az adatvédelmi hatásvizsgálat felülvizsgálatához, valamint az incidenskezeléshez.

A Biztonsági Igazgatóság Információbiztonsági szakterülete, feladatkörében,
– éves tervben meghatározott, vagy
– biztonsági eseményre reagálva, vagy
– a technológia fejlődéséből adódóan ismerté vált sérülékenységekre reagálva,

ellenőrzéseket végez.

Amennyiben adatbiztonsági szempontból hiányosságokat állapít meg, felhívja az adatkezelő figyelmét a szabálytalanságok megszüntetésére, amelynek megvalósulásához szakmai segítséget nyújt.

Az Adatvédelmi tisztviselő, vagy az Adatkezelő szervezeti egység kérésére az adatvédelmi incidens kivizsgálásában és mérlegelésében - amennyiben az adatbiztonsági szakmai kérdést érint - a Biztonsági igazgatóság információbiztonsági szakterülete szakmai segítséget kell, hogy nyújtson.

4.4.4 Informatika szervezet

Az Adatvédelmi tisztviselő, vagy az Adatkezelő szervezeti egység kérésére az adatvédelmi incidens kivizsgálásában és mérlegelésében - amennyiben az informatikai szakmai kérdést érint – az Informatika szervezet szakmai segítséget kell, hogy nyújtson.

4.5 Az adatkezelés lezárása

4.5.1 Az Adatkezelő szervezeti egység feladata

Amennyiben az Adatkezelő szervezeti egység az adatkezeléssel járó tevékenységét megszünteti, döntenie-, és gondoskodnia kell arról, hogy az adatok végleges törlésre és/vagy archiválásra és/vagy anonimizálásra kerüljenek.

Az Adatkezelő szervezeti egységnek dokumentálnia (3. sz. melléklet) kell az adott adatkezelés lezárásának tényét, és ezt meg kell küldenie az Adatvédelmi tisztviselőnek.

4.5.2 Az Adatvédelmi tisztviselő feladata

Az Adatkezelő szervezeti egység által megküldött (3. sz. melléklet) Belső adatvédelmi nyilvántartásba bejelentő lap adatait át kell, hogy vezesse a Belső adatvédelmi nyilvántartásban.

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 (2016. április 27.) 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,
- Magyarország Alaptörvénye,
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.),
- Az Európai Adatvédelmi Testület (korábban: WP29-es munkacsoport), és a Nemzeti Adatvédelmi és Információszabadság Hatóság által elfogadott vélemények, ajánlások, tájékoztatók és közlemények,
- Mt. a munka törvénykönyvéről szóló 2012. évi I. törvény
- Ptk. a polgári törvénykönyvről szóló 2013. évi V. törvény
- 48/2016. (X. 12. MÁV-START Ért. 34.) sz. vezérigazgatói utasítás a MÁV - START Zrt. Informatikai Biztonsági Szabályzatáról
- 71/2018. (XII. 20. MÁV-START Ért. 42.) sz. vezérigazgatói utasítás a MÁV-START Zrt. képzési tevékenységéről

5.2 Módosítások

Nincsenek.

5.3 Hatályon kívül helyezések

Az utasítás hatályba lépésével egyidejűleg hatályát veszti a MÁV-START Zrt. Adatvédelmi Szabályzatáról szóló 24/2014. (II. 12. MÁV-START Ért. 9.) 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 közzététel napján lép hatályba és visszavonásig érvényes.

7.0 MELLÉKLETEK

1. számú melléklet
„Adatvédelmi hatásvizsgálat” mintája

2. számú melléklet
„Érdekmérlegelési teszt” mintája

3. számú melléklet
„Belső adatvédelmi nyilvántartásba bejelentő lap” mintája

4. számú melléklet
„Adatkezelési tájékoztató” mintája

5. számú melléklet
„Adatvédelmi Incidens nyilvántartás” mintája

6. számú melléklet
„Az Adatvédelmi tisztviselő tevékenységének nyilvántartása” mintája

Kerékgyártó József s.k.
vezérigazgató

Adatvédelmi hatásvizsgálat

1. Projektnév, szerepkörök:
Projektnév, 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 határozza meg a tárolás időtartamát, a 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?

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

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* - *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. Mentés, archiválás, megőrzés *(Adatkezelő szervezeti egység tölti ki)*

7.1 Elévülés, lejárat:	
7.2 Archiválás:	
7.3 Alkalmazott védelmi eljárások	

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

8.1 Adathordozó típusa:	
8.2 Tárolás helye:	

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

9.1 Törlés / anonimizálás dátuma:	

Adatkezelési tájékoztató
…….
(*adatkezelési tevékenység megnevezése***)**

1. Az adatkezelő(k) megnevezése

Név:	**MÁV-START Vasúti Személyszállító Zártkörűen Működő Részvénytársaság**
Székhely:	1087 Budapest, Könyves Kálmán krt. 54-60.
Cégjegyzékszám:	Cg. 01-10-045551
A bejegyző bíróság megnevezése:	Fővárosi Törvényszék Cégbírósága
Adószám:	13834492-2-44
E-mail:	(*az Adatkezelő szervezeti egység elérhetősége*)
Adatvédelmi tisztviselő elérhetősége:	(*az Adatvédelmi tisztviselő elérhetősége*)

2. Az adatkezelés célja, jogalapja, módja, kezelt adatok köre és a tárolás időtartama, személyes adatok megismerésére jogosultak köre, az adatok forrása:

Az adatkezelés célja:
A kezelt adatok köre:
Az adatkezelés jogalapja:
(Amennyiben az adatkezelés jogalap a GDPR 6. cikk (1) bekezdésének f) pontja, úgy a jogos érdek kifejtése)
Az adatkezelés időtartama:
Az adatkezelés módja:
(automatizált döntéshozatal esetén annak ténye, ideértve a profilalkotást is, 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)
Az adatok forrása:

3. A személyes adatok megismerésére jogosultak köre:

4. Adatfeldolgozás címzettjei (adatfeldolgozók):

Név:
Székhely:
Cégjegyzékszám:
A bejegyző bíróság megnevezése:
Adószám:
E-mail:
Adattárolás helye:
Adatfeldolgozó tevékenységének leírása:

(harmadik országba történő adattovábbítás esetén, annak ténye, valamint a GDPR-ban meghatározott egyéb körülmények)

5. Adatbiztonsági intézkedésekről szóló tájékoztatás

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)	

Az Adatvédelmi tisztviselő tevékenységének nyilvántartása

Sorszám	Dátum	Tevékenység típusa	Tevékenység leírása	Keletkezett dokumentumok / iktatószámok

Az Adatvédelmi tisztviselő tevékenységének nyilvántartása

Statisztikai adatok:

Tevékenység	db szám
Előző hónap végén a Belső adatvédelmi nyilvántartásban szereplő adatkezelések összesített száma:	
A hónapban a Belső adatvédelmi nyilvántartásba újonnan regisztrált adatkezelések száma:	
Előző hónap végén a tárgyévben történt adatvédelmi incidensek összesített száma:	
A hónapban történt adatvédelmi incidensek száma:	
Folyamatban lévő Hatósági adatvédelmi eljárások száma:	
Folyamatban lévő Hatósági adatvédelmi vizsgálatok száma:	

Szerkeszti: MÁV-START Zrt. Kabinet

Felelős kiadó: Kerékgyártó József vezérigazgató