**A minősített adatok védelmének jogi alapjai**

**A minősített adatok védelmének jogi megalapozása**

Az Alkotmány 61.§ (1) bekezdése alapvető jogként fogalmazza meg a **közérdekű adatok megismeréséhez** és terjesztéséhez való jogot. A közérdekű adatok nyilvánossága és megismerhetősége gyakran a szabad véleménynyilvánításhoz való jog gyakorolhatóságának előfeltételeként jelenik meg.

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló **1992. évi LXIII. törvény (Avtv.)** az állami vagy helyi önkormányzati feladatot, illetve egyéb közfeladatot ellátó szerv számára kötelezettségként fogalmazza meg a kezelésükben lévő közérdekű adatok **bárki általi megismerhetőségének** biztosítását.

Az Avtv. arra is felhatalmazást ad, hogy a törvény honvédelmi, nemzetbiztonsági, bűnüldözési, bűnmegelőzési stb. érdekből **korlátozza** a közérdekű adatok nyilvánosságát.

A közérdekű adatok nyilvánosságával szemben támasztott legerősebb korlátozás azonban az adat **minősítésének** – közkeletű, ámde pontatlan kifejezéssel élve, „titkosításának” - intézménye.

Az adatok ezen körének védelme csak szigorú törvényi előírások mellett valósulhat meg. A **minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.),** illetve a végrehajtásáról rendelkező három kormányrendelet ezeket a törvényi előírásokat hivatott megállapítani.

**A Mavtv. előtti jogi szabályozás rövid áttekintése 1945-től**

Az 1945. és 1990. közötti időszak titokvédelmi szabályozásának általános jellemzője volt a minősítési jogosultság széles körű engedélyezése és rendkívül alacsony szintre való telepítése, illetve a törvényi szint alatti szabályozás.

**A minősített adat védelméről szóló 2009. évi CLV. törvény elfogadása**

Az új szabályozás kialakításakor alapelvként fogalmazódott meg, hogy nemzeti minősített adatvédelmi rendszerünk nem lehet másodlagos a külföldi minősített adatok védelmének rendszeréhez képest.

A Parlament 2009. december 14-én tartott ülésén fogadta el a minősített adat védelméről szóló 2009. évi CLV. törvényt (Mavtv.). A törvény 2010. április 1-jén lépett hatályba.

A Mavtv. felhatalmazása alapján, a törvény végrehajtása érdekében a Kormány az alábbi három rendeletet alkotta meg:

* a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III.26.) Korm. rendelet;
* az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III.31.) Korm. rendelet;
* a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V.6.) Korm. rendelet.

A törvény hatálybalépésével megszűnt az államtitok és a szolgálati titok fogalma. Nemzeti minősített adataink esetében a Mavtv. bevezette a **négyszintű minősítési rendszert**; ily módon **„Szigorúan titkos!”**, **„Titkos!”**, **„Bizalmas!”**, valamint **„Korlátozott terjesztésű!”** minősítési szinteket különböztetünk meg. Ezek a megnevezések természetesen már eddig sem voltak ismeretlenek, azonban az utóbbi három minősítési szint a korábbiakban mint a szolgálati titok egyes fajtái léteztek.

A **minősítési eljárással** kapcsolatban fontos változás, hogy megszűnt az automatizmusokra lehetőséget adó államtitokköri jegyzék, illetve szolgálati titokköri jegyzék.

A „Szigorúan titkos!” és „Titkos!” minősítési szintű adat esetében legfeljebb 30 év lehet az érvényességi idő. Ugyanez „Bizalmas!” minősítési szint esetében 20 év, „Korlátozott terjesztésű!” minősített adat esetén pedig 10 év. Az érvényességi idő meghosszabbítására új minősítési eljárás lefolytatásával, rendkívül indokolt esetben van lehetőség.

Nélkülözhetetlen a káralapú minősítés rendszerének gyakorlati szintű elsajátítása, amely viszont egyfajta szemléletváltást igényel a minősítésre jogosultak részéről.

A **Büntető Törvénykönyv** Mavtv. általi módosítása révén azonban ma már egy „Bizalmas!” vagy akár egy „Korlátozott terjesztésű minősítésű adattal való visszaélés is olyan szankciót von maga után, amely kellő elrettentéssel bírhat.

A **minősített adathoz történő hozzáférés** kapcsán a Mavtv. meghatározza, hogy kérdőívhez kötött nemzetbiztonsági ellenőrzés lefolytatása szükséges. „Korlátozott terjesztésű!” minősítési szintű adatok megismerése esetén nemzetbiztonsági ellenőrzés lefolytatása – a nemzetközi gyakorlathoz hasonlóan – nem előírás. Ez esetben is szükség van azonban titoktartási nyilatkozatra és felhasználói engedélyre.

Az új törvény a nemzeti minősített adatok esetében is bevezette a **személyi biztonsági tanúsítvány** intézményét, amely azt igazolja, hogy az elvégzett nemzetbiztonsági ellenőrzés alapján a minősített adatot felhasználó meddig és milyen minősítési szintű adatokhoz férhet hozzá. A betekintési engedély helyébe a tartalmilag lényegében ezzel megegyező **felhasználói engedély** lépett. (A betekintési engedély elnevezés ugyanis félreértésekre adhatott okot, mivel annak birtokosa az esetek túlnyomó többségében nem kizárólag a minősített adatba való betekintésre volt jogosult.)

**A törvény célja, alapelvek**

 A Mavtv. preambuluma a **törvény célját** akként rögzíti, hogy az az alapvető jogok tiszteletben tartása, a Magyar Köztársaság érdekeinek védelme és az állam nemzetközi kötelezettségvállalásainak teljesítése érdekében a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvénnyel, valamint az elektronikus információszabadságról szóló törvénnyel összhangban meghatározza a minősített adat létrejöttével és kezelésével kapcsolatos alapvető rendelkezéseket, a minősítési eljárás és a nemzeti minősített adat felülvizsgálatának rendjét, a minősített adat védelmének általános szabályait, a nemzeti iparbiztonság rendszerének főbb elemeit, és rendelkezzen a minősített adat védelmét ellátó szervekről és személyekről.

A törvény **öt alapelvet** fogalmaz meg, ezek alapvetően a NATO, illetve az EU Biztonsági Szabályzatainak analógiájára kerültek be a jogszabályba. Az alapelvek a következők:

* ***Szükségesség és arányosság elve*** *–* Ennek értelmében a közérdekű adat nyilvánosságához fűződő jogot minősítéssel korlátozni csak a Mavtv.-ben meghatározott feltételek fennállása esetén, a védelemhez szükséges minősítési szinttel és a feltétlenül szükséges ideig lehet.
* ***Szükséges ismeret elve*** - Minősített adatot csak az ismerhet meg, akinek az állami vagy közfeladata ellátásához feltétlenül szükséges. Önmagában valakinek a beosztása, megbízatása, rangja stb. még nem jogosítja fel a minősített adat megismerésére. A nemzetközi terminológiában a szükséges ismeret elve *„need-to-know”* elvként vált ismertté.
* ***Bizalmasság elve*** - A minősített adat illetéktelen személy számára nem válhat hozzáférhetővé vagy megismerhetővé.
* ***Sérthetetlenség elve*** - A minősített adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg. Az arra jogosult személyét meghatározhatja törvény vagy felhasználói engedély.
* ***Rendelkezésre állás elve*** - Biztosítani kell, hogy a minősített adat az arra jogosult személy számára szükség szerint elérhető és felhasználható legyen.

**A minősített adat létrehozása, a minősítési eljárás szabályai**

**Bevezetés**

A közérdekű adatok nyilvánosságának és ezek korlátozásának értelmezéséhez az Alkotmányon túl a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) 19. §-át kell idéznünk, mely szerint:

Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerveknek vagy személyeknek lehetővé kell tenniük, hogy a kezelésükben lévő **közérdekű adatot bárki megismerhesse, kivéve, ha az adatot törvény alapján az arra jogosult szerv minősítette**, illetve ha az nemzetközi szerződésből eredő kötelezettség alapján minősített adat, továbbá, ha a közérdekű adatok nyilvánosságához való jogot - az adatfajták meghatározásával - törvény

* honvédelmi;
* nemzetbiztonsági;
* bűnüldözési vagy bűnmegelőzési;
* központi pénzügyi vagy devizapolitikai érdekből;
* külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra;
* bírósági vagy közigazgatási hatósági eljárásra tekintettel

korlátozza.

A minősített adatok védelméről szólva azonban egy gyakori félreértést is tisztáznunk kell. Az Avtv. 19/A. § (1)-(2) bekezdése szerint az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló adat a keletkezésétől számított tíz évig nem nyilvános. Ezen adatok megismerését az azt kezelő szerv vezetője engedélyezheti.

A fenti **„Nem nyilvános” jelöléssel ellátott adatok** nem tartoznak a minősített adatok körébe.

A fentieken kívül számos „titokfogalom” létezik a magyar jogrendszerben.

A Polgári Törvénykönyvről szóló 1959. évi IV. törvény szerint létezik **üzleti titok.**

Gyakran találkozunk még a **banktitok** fogalmával. A hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. Törvényben.

Az egészségügyről szóló 1997. évi CLIV. törvény meghatározza, az

**orvosi titok** fogalmát.

Az ügyvédekről szóló 1998. évi XI. törvény az **ügyvédi titok** fogalmát mondja ki.

A Mavtv. az említett titokfajták védelmét és ezek kezelésének rendjét nem szabályozza, nem is teheti, hiszen ezek jobbára a természetes személy valamilyen életviszonyával (egészségügyi állapotával, vagyoni helyzetével stb.) függenek össze.

A Mavtv. célja ellenben, hogy meghatározza az „állam” által keletkeztetett minősített adat létrejöttével és kezelésével kapcsolatos alapvető rendelkezéseket.

**Összefoglalva**: a „Nem nyilvános” jelöléssel ellátott adatokra, az üzleti titokra, az orvosi titokra, az ügyvédi titokra stb. nem lehet kiterjeszteni a Mavtv. és végrehajtási rendeleteiben meghatározott személyi, fizikai, dokumentum és elektronikus biztonsági szabályokat.

**A minősítésre jogosultak**

A Mavtv. elsődleges célja **a magasan minősített adatok számának radikális csökkentése.**

A Mavtv. taxatíve meghatározza a **minősítésre jogosultak körét**.

A Mavtv. kizárólag közhatalmi jogosítványokkal rendelkező személyek részére biztosít minősítői jogkört.

**A minősítői jogkör átruházása**

A minősítői joggal rendelkező, közhatalmi jogosítványokkal felruházott személyeknek, illetve a közjogi és közigazgatási szervezetek vezetőinek írásban kell meghatározniuk – az alábbiak szerinti korlátozással – azokat a beosztásokat, amelyek betöltői részére minősítői jogkört biztosítanak.

A Mavtv. szerint a minősítők minősítői jogkörüket írásban

* **„Szigorúan titkos!”** minősítési szintű adat esetén a helyettesükre, valamint a Kormány tagja a közigazgatási államtitkárra és a helyettes államtitkárra,
* **„Titkos!”, „Bizalmas!” és „Korlátozott terjesztésű!”** minősítési szintű adat vonatkozásában az irányításuk alatt álló, közhatalmi jogosítványokkal felruházott szervben vezetői megbízással rendelkezőkre, illetve vezetői beosztásba kinevezettekre

átruházhatják.

Az általános szabály alól meghatározott igazgatási területeken a Mavtv. kivételt tesz.

Ezek a honvédelem, a nemzetbiztonság és a bűnüldözés, vagyis az állam működésének azon területei, ahol a feladatok végrehajtásának gyorsasága a hatékonyság és a siker feltétele, ahol a „normál” minősítési ügymenet nem lenne életszerű.

**A minősítés alapjai**

A minősítésre csak a meghatározott védhető állami érdekek közvetlen sérelme, illetve veszélyeztetése esetén van mód. A korábbi államtitokköri és szolgálati titokköri jegyzékek megszűntek, helyettük a minősítéssel védhető közérdekek köre került meghatározásra. Ezek az alábbiak:

 A Magyar Köztársaság

* szuverenitása, területi integritása,
* alkotmányos rendje,
* honvédelmi, nemzetbiztonsági, bűnüldözési és bűnmegelőzési tevékenysége,
* igazságszolgáltatási, központi pénzügyi, gazdasági tevékenysége,
* külügyi vagy nemzetközi kapcsolatai,
* állami szerve illetéktelen külső befolyástól mentes, zavartalan működésének biztosítása.

Ugyanakkor a minősítéssel védhető közérdekek körébe való tartozás önmagában nem indok a minősítésre.

A minősítésnek objektív alapja van: azért lesz az adat minősített jellegű, mert az adathoz való illetéktelen hozzáférés az állam valamely védhető érdekét ténylegesen károsítja és a kezdeményező, illetve a minősítő ezt a tényt állapítja meg, valamint ezt felismerhetővé teszi.

A fentiek figyelembevételével a Mavtv. szerint az adat minősítéssel csak akkor védhető, ha

*a)* a keletkezett adat a minősítéssel védhető **közérdekek körébe tartozik**,

*b)* az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult számára hozzáférhetetlenné tétele **károsítja a minősítéssel védhető közérdeket**, és

*c)* az adat **nyilvánosságát** és arra feljogosított személyen kívüli megismerhetőségét **meghatározott ideig** korlátozni szükséges.

Az adat minősítéssel csak valamennyi fent említett (a)-c) pontok) feltétel együttes fennállása esetén és csak a legszükségesebb ideig védhető.

A minősítés a kárközpontú minősítési rendszer alapul vételével történik. Ennek lényege, hogy minél nagyobb kárt okoz a minősített adat „illetéktelen kezekbe történő kerülése”, illetéktelen által történő megváltoztatása, annál magasabb szintű személyi, fizikai, adminisztratív és elektronikus biztonsági követelményeknek kell érvényesülniük a védelem során. A kármérték tehát a védelmi intézkedések szintjét határozza meg.

**A minősítési szintek**

Az egyes minősítési szintek alkalmazására az alábbi meghatározást nyújtja a Mavtv.:

Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele

* **rendkívül súlyosan károsítja** a minősítéssel védhető közérdeket, akkor „Szigorúan titkos!”,
* **súlyosan károsítja** a minősítéssel védhető közérdeket, akkor „Titkos!”,
* **károsítja** a minősítéssel védhető közérdeket, akkor „Bizalmas!”,
* **hátrányosan érinti** a minősítéssel védhető közérdeket, akkor „Korlátozott terjesztésű!”

minősítési szintű.

**Az érvényességi idő**

Az érvényességi idő:

* „Szigorúan titkos!” és „Titkos!” minősítési szintű adat esetén legfeljebb **30 év**,
* „Bizalmas!” minősítési szintű adat esetén legfeljebb **20 év**,
* „Korlátozott terjesztésű!” minősítési szintű adat esetén legfeljebb **10 év**

lehet.

A fenti érvényességi idők meghosszabbítására azonban lehetőséget nyújt a Mavtv:

A **„Titkos!” vagy annál magasabb minősítési szintű adat** minősítésének érvényességi ideje új minősítési eljárás lefolytatásával rendkívül indokolt esetben **egy alkalommal, legfeljebb 30 évvel**, illetve a Magyar Köztársaság - magánszemély jogos érdekével szorosan összefüggő - honvédelmi, nemzetbiztonsági, bűnüldözési vagy igazságszolgáltatási érdekére tekintettel **két alkalommal, legfeljebb 30 évvel** meghosszabbítható.

A **„Bizalmas!” vagy „Korlátozott terjesztésű!”** minősítési szintű adat minősítésének érvényességi ideje új minősítési eljárás lefolytatásával rendkívül indokolt esetben **egy alkalommal, legfeljebb 5 évvel**, illetve a Magyar Köztársaság - magánszemély jogos érdekével szorosan összefüggő - honvédelmi, nemzetbiztonsági, bűnüldözési vagy igazságszolgáltatási érdekére tekintettel **két alkalommal, legfeljebb 20 évvel** meghosszabbítható.

Az új minősítési eljárást az érvényességi idő lejárta előtt le kell folytatni. Az érvényességi idő elteltével az adat minősített jellege megszűnik. A minősítés megszűnése után az adat értelemszerűen újból nem minősíthető.

Az érvényességi idő meghosszabbításához az alábbi összefoglaló táblázat nyújt segítséget:

**A minősített adat készítése, a minősítési javaslat**

Nemzeti minősített adat készítése során a készítő az adathordozó első oldalának felső részén:

* a minősítési szintet,
* az érvényességi időt,
* a minősítő nevét és beosztását tünteti fel.

Amennyiben a fentiek jelölését az adathordozó jellege kizárja, azt külön kísérőlapon vagy az elektronikus minősített adattól adminisztratív módon elválaszthatatlan kezelésű elektronikus adatállományban tünteti fel. Külön kísérőlapot kell készíteni például technikai eszköz, objektum minősített adattá történő minősítésekor is. Az elektronikusan kezelt minősített adatok (például ilyen lehet egy digitális fénykép) minősítése során az NBF kormányrendelet adminisztratív módon elválaszthatatlan kezelésű elektronikus adatállományt (lényegében elektronikus formátumú kísérő”lap”ot) ír elő.

Több lapból álló papíralapú adathordozó esetén - elektronikus minősített adat esetén, ha ez technikailag megoldható - a minősítési szint minden egyes, minősített adatot tartalmazó oldalon, annak felső és alsó részének közepén szerepel.

# Az eddigi gyakorlat szerinti minősítési javaslat intézményét a Mavtv. is alkalmazza.

A minősítést az köteles kezdeményezni, akinél az állami vagy közfeladata ellátása során a minősítési feltételeknek megfelelő adat keletkezik.

A minősítendő adat minősítéséhez a kezdeményező személy **indokolással ellátott minősítési javaslatot készít**.

A minősítési javaslatban fel kell tüntetni

* a minősítéssel védhető valamely közérdekre történő hivatkozást,
* a minősítési szintet,
* a minősítés érvényességi idejét és
* a minősítés indokolását.

A minősítési javaslat indokolásának tartalmaznia kell azokat a tényeket és körülményeket, amelyek a minősítést szükségessé teszik. Az indokolás azonban nyilván nem tartalmazhat olyan adatokat, melyeket önmagukban is minősítéssel védeni szükséges. Éppen ezért a lehető legtömörebb és a minősítői döntés elősegítéséhez szükséges legfontosabb információk megadására kell törekedni

A minősítési eljárás alatt álló, minősíthető adatot tartalmazó adathordozót a kezdeményező minősítés céljából a minősítési javaslattal együtt haladéktalanul felterjeszti a minősítőhöz. Nincs annak jelentősége, hogy annál a szervnél, ahol a minősített adat keletkezik van-e a Mavtv. alapján minősítésre jogosult személy, mivel a minősítési javaslatot minden esetben a feladat- és hatáskörrel rendelkező, a Mavtv. alapján minősítésre jogosult személynek kell felterjeszteni

Annak érdekében, hogy a minősítési eljárás időtlenné válása ne vezethessen visszaélésekhez, a minősítőnek a felterjesztés kézhezvételét követő 30 napon belül kell döntenie az adat minősítéséről (a minősítési javaslat kiadmányozásával). Ha a minősítő a határidő lejártáig az adat minősítéséről nem dönt, a nemzeti minősített adat nem jön létre.

Amennyiben **a minősítendő adat a minősítésre jogosult személynél keletkezik**, a fentiekhez hasonlóan indokolással ellátott minősítési javaslatot készít. A minősítési javaslatban ugyanúgy fel kell tüntetni a minősítéssel védhető valamely közérdekre történő hivatkozást, a minősítési szintet és a minősítés érvényességi idejét. A minősítési javaslat indokolásának ugyanúgy tartalmaznia kell azokat a tényeket és körülményeket, amelyek a minősítést szükségessé teszik.

Miután a minősítésre jogosult személy a döntését az előzőekben meghatározott módon írásba foglalta, a minősítési javaslat kiadmányozásával az adatot minősíti.

A nemzeti minősített adatot tartalmazó adathordozó eredeti irattári példányán, vagy - ha ezt az adathordozó jellege kizárja - külön kísérőlapon, vagy az elektronikus minősített adattól adminisztratív módon elválaszthatatlan kezelésű elektronikus adatállományban szerepel a minősítési javaslat és a minősítési javaslat tárgyában hozott döntés. A minősítő a döntését saját kezűleg aláírja vagy elektronikus aláírásával látja el.

A minősítési eljárás alatt álló adatot a minősítő döntéséig a kezdeményezett minősítési szintre vonatkozó személyi, fizikai, adminisztratív és elektronikus biztonsági szabályok szerint kell kezelni.

A nemzeti minősített adat a minősítő által történő minősítéssel jön létre.

A minősített adat kezelése során mindig egyértelműen felismerhetőnek kell lennie az adat minősített jellegének. A nemzeti minősített adat létrejöttéhez a minősítési jelölés formai követelményeit is be kell tartani, vagyis minden esetben fel kell tüntetni a nemzeti minősített adat hordozóján vagy ha arra nincs lehetőség külön kísérőlapon

* a minősítési szintet („Szigorúan titkos!”, „Titkos!”, „Bizalmas!”, Korlátozott terjesztésű!”),
* az érvényességi időt,
* a minősítő nevét és beosztását.

A minősítő határozza meg, hogy a minősített adatot tartalmazó adathordozóból hány példány készüljön.

A minősítő által meghatározott példányszámon felül a minősítő engedélye vagy hozzájárulása nélkül további példányt készíteni nem lehet.

A minősített adat készítése során az adathordozó tartalmazza a:

* a minősítési szintet („Szigorúan titkos!”, „Titkos!”, „Bizalmas!”, Korlátozott terjesztésű!”), több lapból álló papíralapú adathordozó esetén - elektronikus minősített adat esetén, ha ez technikailag megoldható - a minősítési szintet minden egyes minősített adatot tartalmazó oldalon, annak felső és alsó részének közepén
* az érvényességi időt,
* a minősítő nevét,
* a minősítő beosztását,
* a készítő szerv megnevezését,
* a példányszámot,
* a példánysorszámot,
* elektronikus minősített adat esetét kivéve az adathordozó terjedelmét,
* a mellékletek esetén azok
	+ darabszámát,
	+ példánysorszámát,
	+ terjedelmét és
	+ az adathordozótól eltérő szintű minősítés esetén minősítési szintjét,
* a kiadmányozás dátumát,
* az eredeti irattári példány esetében a kiadmányozó aláírását, elektronikus minősített adat esetén elektronikus aláírását.

A nemzeti minősített adatot tartalmazó adathordozó eredeti irattári példányán, vagy - ha ezt az adathordozó jellege kizárja - külön kísérőlapon, vagy az elektronikus minősített adattól adminisztratív módon elválaszthatatlan kezelésű elektronikus adatállományban szerepel a minősítési javaslat és a minősítési javaslat tárgyában hozott döntést

Az egyes példányok címzettjeinek felsorolását az irattári példányhoz csatolt - az egyes címzettek részére továbbított példány sorszámát is tartalmazó - külön elosztó tartalmazza. Az egyes példányok címzettjeit - külön elosztó helyett - az adathordozó is tartalmazhatja.

Amennyiben a fentiekben meghatározottak feltüntetésére az adathordozó jellege miatt nincs mód, akkor azokat külön kísérőlap vagy az elektronikus minősített adattól adminisztratív módon elválaszthatatlan kezelésű elektronikus adatállomány tartalmazza.

A minősítő a minősítéssel egyidejűleg **a minősített adat különleges kezeléséről** is rendelkezhet és a minősített adat hordozóján - ha ezt az adathordozó jellege kizárja, akkor külön kísérőlapon vagy az elektronikus minősített adattól adminisztratív módon elválaszthatatlan kezelésű elektronikus adatállományban - valamint annak csomagolásán a következő különleges kezelési utasításokat alkalmazhatja:

* „Saját kezű felbontásra!”,
* „Más szervnek nem adható át!”,
* „Nem sokszorosítható!”,
* „Kivonat nem készíthető!”,
* „Elolvasás után visszaküldendő!”,
* „Zárt borítékban tárolandó!”,
* „Különösen fontos!”.

A fentieken kívül bármilyen más, a minősített adat sajátosságától függő különleges kezelési utasítás feltüntethető.

A különleges kezelési utasítástól csak a minősítő írásbeli engedélyével lehet eltérni.

Ha több minősített adat el nem különíthető módon, csak együttesen kezelhető (pl.: dossziékban történő minősített adatok kezelése), akkor azokat az abban szereplő legmagasabb minősítési szintnek megfelelően kell kezelni.

Nemzetközi szerződés vagy megállapodás alapján készített nemzeti minősítést igénylő adat minősítése a fent leírtak szerint történik. Ilyen adat külföldre történő továbbítása előtt a minősítési szintet magyarul, valamint a nemzetközi szerződésben vagy megállapodásban meghatározott nyelven - az Európai Unió intézményei és szervei tekintetében angolul vagy franciául - is fel kell tüntetni.

**A minősítési jelölés megismétlése**

A Mavtv. lehetőséget teremt arra, hogy **ne kelljen új minősítési eljárást lefolytatni**, ha a készített adatba saját vagy más minősítő által korábban készített minősített adatot is belefoglalnak, és ennek során további, saját minősítést igénylő adat nem keletkezik. Ebben az esetben a korábban készített minősített adat minősítési jelölését (a minősítési szintet, az érvényességi időt, a minősítő nevét és a minősítő beosztását) meg kell ismételni, kivéve ha azt a megismételni kívánt adat minősítője megtiltotta.

Ha a megismételt minősítésű jelölésű adat mellett további, saját minősítést igénylő adat is keletkezik, akkor arra az adatra a minősítési eljárást le kell folytatni.

Megismételt minősített adat készítése során a készítő a megismételt minősítési jelölést az adathordozó első oldalának felső részén vagy - ha ezt az adathordozó jellege kizárja - külön kísérőlapon vagy az elektronikus minősített adattól adminisztratív módon elválaszthatatlan kezelésű elektronikus adatállományban tünteti fel.

**A biztonsági feltételek megteremtése**

A Mavtv.-ben foglaltak szerint minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a minősített adat védelméhez szükséges, az adat minősítési szintjének megfelelő, a Mavtv-ben és a végrehajtására kiadott rendeletekben meghatározott **személyi, fizikai, adminisztratív és elektronikus biztonsági feltételeket**. A biztonsági feltételek megteremtéséért **a minősített adatot kezelő szerv vezetője** tartozik felelősséggel.

**Az adatkezelési és a rendszerengedélyezési eljárás**

A Mavtv. által bevezetett, új engedélyezési eljárás lényege, hogy 2010. április 1-je óta a Magyar Köztársaság területén a minősített adatot kezelő állami vagy gazdálkodó szerveknél csak a **Nemzeti Biztonsági Felügyelet által kiállított engedélyek alapján** lehet minősített adatot **papír alapú vagy elektronikus adathordozón** kezelni.

**A személyi biztonsági intézkedések**

A biztonsági vezetőnek úgy kell a minősített adatvédelem személyi biztonsági rendszerét működtetnie, hogy minősített adathoz – a Mavtv-ben meghatározott kivételekkel – kizárólag

a) **személyi biztonsági tanúsítvánnyal** (és a kiadásához szükséges nemzetbiztonsági ellenőrzéssel és az ezt igazoló érvényes szakvéleménnyel)

b) **felhasználói engedéllyel** és

c) **titoktartási nyilatkozattal** rendelkező jogosult felhasználó, a felhasználói engedélyben meghatározott rendelkezési jogosultságokkal férhessen hozzá.

**A minősített adatvédelmi rendszer működtetésében részt vevő személyek**

A minősített adatvédelem helyi működtetéséhez szükséges, megfelelő képesítési követelményekkel és szakmai ismeretekkel és rendelkező személyzet létszámának meghatározása és folyamatos biztosítása a minősített adatot kezelő szerv vezetőjének felelőssége.

**A biztonsági vezető és a helyi biztonsági felügyelet**

A minősített adatot kezelő szervnél a *minősített adat védelmével* kapcsolatos **feladatok** **végrehajtását** és **koordinálását** a minősített adatot kezelő szerv vezetője által kinevezett biztonsági vezető végzi.

**Nem szükséges függetlenített**, csak erre a feladatra specializált – más szakmai területtel nem foglalkozó – **biztonsági vezetőt kinevezni**, de az **egyszemélyi felelősség elvének** érvényesülésével kell ellátnia a biztonsági vezetői feladatokat.

Biztonsági vezetőt a minősített adatot kezelő szervnél csak az érintett szervnél meglévő munkaviszony vagy munkavégzésre irányuló egyéb jogviszony fennállása esetén lehet kinevezni. Biztonsági vezetői feladat **megbízási szerződés alapján nem** végezhető.

A biztonsági vezető a minősített adatot kezelő szervnél egyidejűleg titkos ügykezelői munkakörben nem foglalkoztatható.

A törvény által meghatározott elnevezés is arra utal,hogy célszerű a minősített adatot kezelő szerveknél vezetői beosztást betöltő, sőt a szervezeti hierarchia felső szintjén lévő **vezetői beosztásban** lévő személyt kinevezni erre a feladatra, annak érdekében, hogy a szerv vezetőjétől kapott jogkörben eljárva a minősített adat védelmével kapcsolatos döntéseinek, akaratának akár utasítási joggal érvényt tudjon szerezni. Erre kevés az esélye a „súlytalan”, a minősített adatot kezelő szerven belül sem érdekérvényesítő képességgel, sem utasítási joggal, sem vezetői tekintéllyel nem rendelkező munkatársnak.

**A biztonsági vezető és a helyi biztonsági felügyelet feladatai**

**Szabályalkotás**

a) Elkészíti **a biztonsági szabályzatot**, majd annak kiadmányozását követően gondoskodik a biztonsági szabályzat naprakész állapotban tartásáról és betartatásáról.

b) Intézkedik arról, hogy **a reagáló erő számára** a biztonsági területtel és az adminisztratív zónával kapcsolatos **feladatok írásban** kerüljenek meghatározásra.

**Ellenőrzés**

Minden év **február 28-ig** jegyzőkönyv felvétele mellett intézkedik a minősített adat védelmére vonatkozó személyi, fizikai, adminisztratív **biztonsági rendelkezések** megtartásának **belső ellenőrzéséről**, ennek keretében ellenőrzi a minősített adatot kezelő szervnél kezelt nemzeti és külföldi minősített adatok felhasználását és tárolását; továbbá gondoskodik **az előző évi iratforgalmi statisztika** minősítési szintenkénti bontásban történő **elkészítéséről**.

**A személyi biztonság körébe tartozó feladatok**

**Az állami** szerv biztonsági vezetőjének hatásköre:

A minősített adatot kezelő állami szerv biztonsági vezetője a nemzeti minősített adatot felhasználó, valamint ilyen adatot felhasználó közreműködő részére egy példányban **kiadja a nemzeti minősített adatra érvényes személyi biztonsági tanúsítványt**. Intézkedik a nemzeti minősített adatra érvényes személyi biztonsági tanúsítványok kezeléséről és tárolásáról. A szükséges biztonsági feltételek hiánya vagy megszűnése esetén a nemzeti minősített adatra érvényes személyi biztonsági tanúsítványt visszavonja, majd a visszavonást követően intézkedik a személyi biztonsági tanúsítvány selejtezéséről.

**Mind az állami szerv, mind a gazdálkodó** **szervezet** biztonsági vezetőjének további hatásköre:

a) **Kezdeményezi** a Nemzeti Biztonsági Felügyeletnél **a külföldi** minősített adatra érvényes **személyi biztonsági tanúsítvány kiadását** a NATO, NYEU és az EU minősített adatokhoz hozzáférő felhasználók és közreműködők részére. Intézkedik a személyi biztonsági tanúsítványok kezeléséről és tárolásáról. A Nemzeti Biztonsági Felügyeletet írásban értesíti, ha az érintett személy tekintetében a szükséges biztonsági feltételek nem állnak fenn és ezt követően intézkedik a külföldi minősített adatra érvényes személyi biztonsági tanúsítvány selejtezéséről.

b) Gondoskodik arról, hogy a **titkos ügykezelő naprakész és pontos információval** rendelkezzen a minősített adatot kezelő szervnél érvényes személyi biztonsági tanúsítvánnyal rendelkező személyekről.

c) Minden rendezvény esetében, ahol NATO, NYEU, valamint EU minősített adatok válnak hozzáférhetővé és ezt a rendezvényre vonatkozó előírások megkövetelik, a **rendezvényen résztvevőnek** a Nemzeti Biztonsági Felügyeletnél nyilvántartásba vett személyi biztonsági tanúsítványáról egy példányban - nemzetközi rendezvény esetén angol nyelvű - **igazolás kiadását kezdeményezi** a Nemzeti Biztonsági Felügyeletnél.

d) A biztonsági vezető felelőssége, hogy az a felhasználó, akinek a feladata ellátásához ez szükséges, felhasználói engedéllyel és általa aláírt titoktartási nyilatkozattal rendelkezzen, kivéve, ha a Mavtv. szerint ilyen engedélyre és nyilatkozatra nincs szükség. Intézkedik a **felhasználói engedély és a titoktartási nyilatkozat kezeléséről,** valamint tárolásáról. A biztonsági vezető felelőssége, hogy a minősített adatot kezelő szervnél tárolt felhasználói engedély és titoktartási nyilatkozat a felhasználói engedély visszavonását követően a visszaélés szigorúan titkos és titkos minősítésű adattal bűncselekményre a büntető törvénykönyvben meghatározott büntetési tétel felső határának megfelelő ideig (15 év) fellelhető legyen. Ezt követően intézkedik ezen okmányok selejtezési jegyzőkönyv felvétele mellett történő megsemmisítéséről.

e) A titkos ügykezelőre meghatározott **tananyag és vizsgakövetelmény elkészíttetése**, az oktatás szervezeti kereteinek és a vizsgáztatás eljárási rendjének meghatározása, valamint a vizsgabizottság kijelölése a szakirányításra jogosult vezető vagy a biztonsági vezető feladata. A titkos ügykezelőre a minősített adatot kezelő szervnél meghatározott tananyagot és a vizsgakövetelményeket előzetes jóváhagyás céljából megküldi a Nemzeti Biztonsági Felügyelet részére. A titkos ügykezelők részére szervezett vizsga tervezett időpontjáról a Nemzeti Biztonsági Felügyelet elnökét előzetesen írásban tájékoztatja.

**A fizikai biztonság körébe tartozó feladatok**

a) Intézkedik a biztonsági területre telepített **biztonságtechnikai eszközöknek** és rendszereknek a gyártó előírása szerinti gyakorisággal, de legalább évente egy alkalommal történő **karbantartásáról.**

b) **Engedélyezi** a személyi biztonsági tanúsítvánnyal rendelkező **látogatók** azonosító kártya viselése melletti önálló, kíséret nélkül **mozgását** a biztonsági területen, amennyiben a biztonsági területre érkező látogató biztonsági vezetője írásban igazolja, hogy a látogató személyi biztonsági tanúsítvánnyal rendelkezik.

c) A biztonsági vezető vagy az általa írásban kijelölt személy **őrzi** a biztonsági tárolók és a **biztonsági terület tartalékkulcsait és kódjait** - a tárolt adatok minősítési szintjének megfelelő - biztonsági tárolóban. A tartalékkulcsok, kódok őrzés céljából a biztonsági vezetőnek vagy az általa kijelölt személynek történő átadása és visszavétele dokumentált módon, az erre a célra megnyitott nyilvántartásban történik.

d) A biztonsági vezető **kezeli** a biztonsági területen használt **kódok megváltoztatásának** tényét és időpontját rögzítő **nyilvántartást**.

**Az adminisztratív biztonság körébe tartozó feladatok**

a) A szakmai alárendeltségébe tartozó **Nyilvántartó(k) és Kezelő pont(ok) szakmai felügyelete.**

b) A más szervtől kapott, valamint a saját készítésű minősített adatot tartalmazó adathordozó, ügyviteli érdeket nem képviselő **többes példánysorszámú** példányai **megsemmisítésének előzetes jóváhagyása**, amennyiben erre a minősített adatot kezelő szerv vezetője felhatalmazta.

c) Minden év **március 10-ig** intézkedik a **NATO és EU** minősített adatok tekintetében lefolytatott **éves ellenőrzés eredményének** és a minősített adatot kezelő szervhez érkezett vagy ott készített NATO és EU minősített adatok **iratforgalmi statisztikájának** minősítési szintenkénti bontásban a **NATO-NYEU Központi Nyilvántartó**, valamint az **EU Központi Nyilvántartó részére** történő megküldéséről.

d) Minden év **március 31-éig** intézkedik a **nemzeti** minősített adatok tekintetében lefolytatott **éves ellenőrzés eredményének** és az előző évben a minősített adatot kezelő szervhez érkezett vagy ott készített nemzeti minősített adatok **iratforgalmi statisztikájának** minősítési szintenkénti bontásban a **Nemzeti Biztonsági Felügyeletre történő** megküldéséről.

**Az elektronikus biztonság körébe tartozó feladatok**

a) **Kezdeményezi a Nemzeti Biztonsági Felügyeletnél** az elektronikus biztonsághoz és a rejtjeltevékenységhez előírt **engedélyek beszerzését** és gondoskodik azok nyilvántartásáról.

b) **Irányítja** a **rendszerbiztonsági felügyelő** vagy a rendszerbiztonsági felügyelet és a **rendszeradminisztrátor** tevékenységét, valamint ellenőrzi az elektronikus biztonsági előírások betartását.

c) Gondoskodik **a rendszerbiztonsági dokumentumok** elkészítéséről.

d) Minden **év február 28-ig** tájékoztatja a Nemzeti Biztonsági Felügyeletet a szervezet **rejtjeltevékenységéről**, a Nemzeti Biztonsági Felügyelet által megadott szempontok alapján.

e) **Irányítja a rejtjelfelügyelő** vagy a rejtjelfelügyelet tevékenységét.

f) Gondoskodik arról, hogy a **rejtjeltevékenységgel** kapcsolatos, védelem alá eső információkat csak azok a személyek ismerhessék meg, akiknek a munkájához az feltétlenül szükséges, és arra a megfelelő engedélyekkel rendelkeznek.

g) Folyamatos **kapcsolatot tart a Nemzeti Hálózatbiztonsági Központtal** a használt rendszerek hálózati biztonsága vonatkozásában.

h) Kivizsgálja **a rendszerbiztonsági eseményeket**.

**A minősített adat biztonságának megsértése esetén elvégzendő feladatok**

A minősített adat biztonságának megsértése esetén intézkedik a minősített adat biztonságának megsértése kapcsán felmerült **kár felméréséről és enyhítéséről**, valamint - ha ez lehetséges - a **jogszerű állapot helyreállításáról**. Itt meg kell jegyeznünk, hogy a Mavtv. nem a biztonsági vezető, hanem a minősített adatot kezelő szerv vezetőjének felelősségi körébe utalja a minősített adat biztonságának megsértésével kapcsolatos tájékoztatási kötelezettséget. Ha a Mavtv-t vagy a végrehajtásáról szóló rendelkezéseket olyan módon sértették meg, hogy a „Szigorúan titkos!”, a „Titkos!”, valamint a „Bizalmas!” minősítési szintű adat ezáltal illetéktelen személy részére hozzáférhetővé válhatott vagy ennek veszélye fennáll, a minősített adatot kezelő szerv vezetője a minősítőt és a Nemzeti Biztonsági Felügyeletet köteles erről tájékoztatni.

**A biztonsági vezető adatkezelése**

A biztonsági vezető és a helyi biztonsági felügyelet a személyi biztonsági tanúsítvány kiadásával összefüggésben az alábbi **adatok kezelésére jogosult** a Mavtv. felhatalmazása alapján:

*a)* az érintett személy

*aa)* természetes személyazonosító adatai,

*ab)* állampolgársága,

*ac)* úti okmányának okmányazonosítója,

*ad)* minősített adat felhasználásához kötődő munkahelye, beosztása és feladatköre,

*ae)* a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott biztonsági kérdőívben és szakvéleményben foglalt adatai,

*b)* a kiadott személyi biztonsági tanúsítvány száma, kelte, érvényességi ideje és szintje.

A biztonsági vezető ezeket az adatokat az érintett személy részére kiadott utolsó személyi biztonsági tanúsítvány érvényességi idejének lejártát vagy visszavonását követő 8 évig kezelheti, utána megsemmisítésükről, törlésükről gondoskodnia kell.

**A rendszerbiztonsági felügyelő, a rendszerbiztonsági felügyelet és a központi rendszerbiztonsági felügyelet**

A minősített adat **elektronikus rendszeren** való kezelése esetén – az elektronikus biztonságról a későbbiekben lesz még szó – a szerv vezetőjének **rendszerbiztonsági felügyelőt** kell kijelölnie.

A rendszerbiztonsági felügyelő a biztonsági vezető irányítása alatt a rendszer alkalmazási területén felelős a minősített adatot kezelő **elektronikus rendszer** személyi, fizikai, adminisztratív, valamint rendszerbiztonsági feltételeinek teljesüléséért, a biztonsági beállítások és hozzáférési jogosultságok beállításáért.

A rendszerbiztonsági felügyelői feladatokat a biztonsági vezető is elláthatja.

**A rendszeradminisztrátor**

A minősített adatot elektronikus rendszeren kezelő szerv vezetője **rendszeradminisztrátort** jelöl ki. A rendszeradminisztrátor a rendszerbiztonsági felügyelő irányítása mellett a **rendszer üzemeltetéséért, karbantartásáért** felelős személy.

**A rejtjelfelügyelő és a (központi) rejtjelfelügyelet**

Rejtjeltevékenységet folytató szerv vezetője köteles **rejtjelfelügyelőt** kijelölni vagy - amennyiben a minősített anyagok mennyisége indokolja - rejtjelfelügyeletet létrehozni.

**A rejtjelző**

A rejtjelező a rejtjelfelügyelő irányítása mellett a rejtjelző tevékenység végrehajtásáért felelős személy.

**A Nyilvántartó, a Kezelő pont és a titkos ügykezelő**

A **Nyilvántartó** és a **Kezelő pont** a minősített adatot kezelő szerv olyan szervezeti egysége, amely a minősített adatot kezelő szervhez érkező vagy ott keletkező **minősített adatok** **nyilvántartásával kapcsolatos feladatokat** hajtja végre, tevékenységét a **biztonsági vezető** **szakmai alárendeltségében** végzi. A szakmai alárendeltség nem jelenti egyben a szervezeti alárendeltséget is, bár a gyakorlatban a legtöbbször azonos szervezeti egységnél találjuk a biztonsági vezetőt és a Nyilvántartót. A Nyilvántartót üzemeltető minősített adatkezelő szerv létrehozhat a Nyilvántartó ellenőrzése alatt álló Kezelő pontot, amelynek nyilvántartással kapcsolatos feladatai a szerv vezetőjének döntése alapján teljesen vagy csak részben egyeznek meg a Nyilvántartóéval, (például amikor a Kezelő pont egyes nyilvántartási tevékenység (pl. megsemmisítés) végzésére nem kap hatáskört). Kezelő pont kizárólag a Nyilvántartó alárendeltségében hozható létre.

A minősített adatot kezelő szervnél egyidejűleg több Nyilvántartó és Kezelő pont is kialakítható és működtethető.

**Nyilvántartó** működtetéséhez minimálisan **két fő**, a **Kezelő pont** működtetéséhez **egy fő** **titkos ügykezelő** kinevezése, továbbá **egy fő helyettesítéssel** megbízott titkos ügykezelő írásban történő kijelölése szükséges.

**A titkos ügykezelő feladatai**

A titkos ügykezelő feladatairól az NBF kormányrendelet rendelkezik:

a) a minősített adat **átvétele,** minősített küldemény **felbontása,**

b) a minősített adat **iktatása, tárolása**,

c) a minősített adat szerven belül történő **átadása és visszavétele,**

d) a minősített adat szerven kívüli **továbbításának előkészítése**,

e) a **felhasználói jogosultság megszűnése** esetén a minősített adat **visszavétele,**

f) a minősített adat kezeléséhez szükséges **iratkezelési segédletek** főnyilvántartó könyvben történő **nyilvántartásba vétele és megnyitása,**

g) a minősített adat belföldre, valamint **külföldre történő továbbításához** szükséges iratkezelési feladatok végrehajtása,

h) a minősített adat birtokban tartása,

i) a minősített adatot tartalmazó adathordozó **megsemmisítésének előkészítése** és az abban történő részvétel.

Titkos ügykezelő az lehet, aki legalább **középfokú iskolai végzettséggel**, a kezelt minősített adatok minősítési szintjének megfelelő szintű **személyi biztonsági tanúsítvánnyal** és **felhasználói engedéllyel** rendelkezik, aláírta a **titoktartási nyilatkozatot**, a minősített adat védelmére vonatkozó rendelkezések, így különösen a Mavtv. és a végrehajtására kiadott rendelet ismeretéből, gyakorlati alkalmazásából sikeres **vizsgát tett**, továbbá erre a feladatra a minősített adatot kezelő szerv vezetője **írásban** **kinevezte**.

A titkos ügykezelő a minősített adatot kezelő szervnél **egyidejűleg biztonsági vezetővé nem nevezhető ki.**

**A fizikai biztonsági intézkedések**

**A fizikai biztonság alapelvei és követelményei**

Minden olyan **helyiséget, épületet, építményt**, ahol minősített adatot kezelnek, **fizikai biztonsági intézkedésekkel** kell védeni az arra nem jogosult személyeknek a minősített adathoz történő hozzáférése ellen.

A minősített adat felhasználására és tárolására szolgáló helyszín fizikai biztonsági rendszerének több egymásra épülő elemből kell állnia. Ez az ún. **körkörös védelem elve**, mely szerint a minősített adatok fizikai védelmét külső, közbenső és belső fizikai biztonsági elemeknek együttesen kell biztosítaniuk. A fizikai biztonság

a) külső elemei a védendő terület határait biztosítják,

b) közbenső elemei észlelik az illetéktelen behatolást és riasztják a reagáló erőt,

c) belső elemei a reagáló erő megérkezéséig késleltetik az illetéktelen behatolót a minősített adatokhoz történő hozzáférésben.





**Belső elemek**









**Közbenső elemek**

**Külső elemek**



Hangsúlyozni kívánjuk, hogy a nemzeti minősített adatokra előírt korábbi jogi szabályozással ellentétben az NBF kormányrendelet **kötelezővé teszi** mind a **mechanikai, mind az elektronikai védelem** eszközeinek egyidejű kiépítését és működtetését, mivel ezek az eszközök **nem helyettesítik, hanem kiegészítik egymást**:

* a *mechanikai védelem* eszközei *fizikai gátat képezve akadályozzák*, illetve *késleltetik* a védett helyiségbe, területre történő illetéktelen *behatolást,* valamint a minősített adatotokhoz történő illetéktelen *hozzáférést;*
* az *elektronikai védelem* eszközei *észlelik az illetéktelen behatolást*, és *riasztják a reagáló erőket.*

További fontos szempont a minősített adatok kezelésének **zónaszerű, centralizált kiépítése**, ami a védelem koncentrációja miatt nem csak a minősített adathordozók biztonságát növeli, hanem a költségeket is csökkenti.

A fizikai biztonsági rendszerben **csak garantált minőségű** biztonságtechnikai eszközök használhatók. Ennek igazolására a Nemzeti Biztonsági Felügyelet elfogadja a gyártó által beszerzett, a **termék megfelelőségéről kiadott igazolást** és a nemzetközi gyakorlatban ezzel egyenértékű okiratot.

**A biztonsági terület és az adminisztratív zóna**

A **„Bizalmas!” vagy ennél magasabb** minősítési szintű minősített adat az alábbiakban felsorolt három kivételtől eltekintve kizárólag **I. vagy II. osztályú biztonsági területen** használható fel és tárolható.

A biztonsági területen kívül is felhasználható, de nem tárolható:

1. katonai, nemzetbiztonsági és bűnügyi műveletekben a technikai eszköz és a minősített adat,
2. az Országház épületében a minősített adat,
3. munkaidőben papír alapú minősített adathordozó az adminisztratív zónában.

**I. osztályú biztonsági területnek** minősül minden olyan helyszín, ahol „Bizalmas!” vagy annál magasabb minősítési szintű minősített adatot használnak fel, vagy használnak fel és tárolnak, vagy tárolnak olyan módon, hogy a területre való **belépés** egyben a minősített adathoz való **hozzáférést** is jelenti. A terület **fizikailag körülhatárolt és védett**, valamint a **ki- és belépés ellenőrzött**. A **ki- és belépés csak** beléptető rendszeren keresztül és csak azon személyek számára engedélyezhető, akik erre külön felhatalmazással és **személyi biztonsági tanúsítvánnyal** rendelkeznek.

**II. osztályú biztonsági területnek** minősül minden olyan helyszín, ahol „Bizalmas!” vagy annál magasabb minősítési szintű minősített adatot használnak fel, vagy használnak fel és tárolnak, vagy tárolnak olyan módon, hogy az illetéktelen hozzáférést belső intézkedésekkel meg lehet akadályozni. A terület **fizikailag körülhatárolt és védett**, valamint **a ki- és belépés ellenőrzött** és a minősített adatokhoz történő illetéktelen hozzáférés megakadályozása érdekében a biztonsági területre csak külön felhatalmazással lehet belépni. **Személyi biztonsági tanúsítvánnyal nem** **rendelkező** személy **csak kísérettel** léphet be.

A biztonsági területen belül a nemzeti és külföldi „Bizalmas!” vagy ennél magasabb minősítési szintű minősített adatokat egymástól elkülönítve kell tárolni.

**Az I. osztályú biztonsági terület helyszíne (a minősített adat nyílt tárolása)**

**Nyílt tárolás** esetén a biztonsági terület kialakítására az NBF kormányrendelet rendkívül **szigorú.**

**A II. osztályú biztonsági terület helyszíne (a minősített adat zárt tárolása)**

A **zárt tárolásra** az NBF kormányrendelet un. **mátrixos pontszámítást** alkalmaz.

Ennek lényege, hogy az NBF kormányrendeletben felsorolt valamennyi **fizikai biztonsági intézkedéshez egy-egy pontszám** tartozik, továbbá az NBF kormányrendelet 2. és 3. számú melléklete meghatározza a nemzeti és a külföldi minősített adatokra minősítési szintenként meghatározott **minimum pontszámot**. Ez alapján az adatkezelés engedélyezését végző Nemzeti Biztonsági Felügyelet és az engedélyt kérő szerv is ki tudja számolni a biztonsági területen **alkalmazott fizikai biztonsági intézkedések** **együttes pontszámát**, amely megmutatja azt, hogy az engedélykérelemmel érintett helyszín milyen minősítési szintű adatok kezelésére alkalmas.

A **II. osztályú biztonsági terület helyszínét** a mechanikai védelem erőssége alapján az NBF kormányrendelet **négy kategóriába** sorolja. A négy kategória esetében **eltérő erősségű mechanikai védelemmel** rendelkező helyszíneket találunk:

**Az adminisztratív zóna**

A **„Korlátozott terjesztésű!”** minősítési szintű minősített adat biztonsági területen kívül **adminisztratív zónában is** **felhasználható** és az adminisztratív zónán belül **zárható** *irodabútorban vagy lemezszekrényben* is **tárolható.**

Adminisztratív zónának minősül minden olyan helyszín, ahová **a belépés ellenőrzött**. A biztonsági terület körül adminisztratív zóna is kiépíthető.



**Az adminisztratív biztonsági intézkedések alapelvei és követelményei**

Az **adminisztratív biztonsági intézkedések** a minősített adat

a) nyomonkövethetőségét,

b) bizalmasságát,

c) sérthetetlenségét és

d) rendelkezésre állását biztosítják.

Az egyik legfontosabb adminisztratív biztonsági feladat az, hogy a minősített adatok nyilvántartására szolgáló hiteles és a felelősség megállapítására alkalmas nyilvántartási rendszert úgy kell kialakítani és működtetni, hogy biztosítva legyen a *minősített adatoknak a szerven belül történő* **mozgásának nyomonkövethetősége.**

A **bizalmasság** megtartása azt jelenti, hogy bárki, aki jogszerűen jutott a minősített adat birtokába, – így különösen a minősítő, a minősítés kezdeményezője, a felhasználó és a nyilvántartási cselekmények végzése során a titkos ügykezelő – köteles úgy eljárni, hogy a birtokába került minősített adat *illetéktelen személy számára ne válhasson hozzáférhetővé vagy megismerhetővé.*

A minősített adat **sérthetetlenségét** – mely szerint az adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg – számos adminisztratív biztonsági szabály garantálja: pl. csak az adat minősítője (vagy jogutódja), illetve a felülbírálatra jogosult dönthet egy adat minősítésének felülvizsgálatáról; csak a minősítő, valamint - a NATO és az EU Szigorúan titkos! minősítési szintű adatokat leszámítva - a címzett engedélyezheti a minősített adat sokszorosítását, fordítását és kivonatolását; kizárólag a minősített adatot kezelő szerv vezetője vagy általa adott felhatalmazás alapján a biztonsági vezető engedélyezheti a más szervtől kapott, valamint a saját készítésű minősített adatot tartalmazó adathordozó, ügyviteli érdeket nem képviselő többes példánysorszámú példányainak megsemmisítését.

Megfelelően működtetett adminisztratív biztonsági rendszer garantálja a minősített adatok **rendelkezésre állását,** vagyis azt,hogy a minősített adatok az *arra jogosult személy részére* bármikor elérhetőek és felhasználhatóak legyenek, a nyilvántartás alapján a minősített adatok *holléte*, *minősítési szintje és érvényességi ideje*, valamint *mennyisége* bármikor megállapítható és azonosítható legyen.

A titkos ügykezelők által a *leggyakrabban használt nyilvántartások* esetében **nem beszélhetünk kötelező formaiságról,** azaz nem létezik a Mavtv-ben vagy az NBF kormányrendeletben kötelezően meghatározott forma, elrendezés, rovatrendszer. A legtöbb minősített adatkezelő szervnél még mindig **a papíralapú nyilvántartás a jellemző**, ami egyrészt pénzügyi-anyagi, másrészt biztonsági természetű (a hitelességgel, hiteles aláírással, illetve annak hiányával kapcsolatos) problémákra vezethető vissza.

*Már több helyen megjelentek* a számítógépen vezetett nyilvántartások – elsősorban az iratkezelési szoftverek részét képező ***elektronikus iktatókönyvek*** – is. Mind a papíralapú, mind az elektronikus iratkezelési szoftverrel szemben követelmény, hogy az NBF kormányrendeletben az adott iratkezelési segédletre **előírt azonosító adatok rögzítésére alkalmas** legyen. Az iratkezelési szoftver használata csak a Nemzeti Biztonsági Felügyelet egyetértésével történhet, melyre akkor kerülhet sor, ha a Nemzeti Biztonsági Felügyelet a vizsgálat során iratkezelési szoftver vizsgálata során megállapítja, hogy az megfelel az NBF kormányrendeletben foglalt adminisztratív, illetve az Elektronikus kormányrendeletben előírt elektronikus biztonsági feltételeknek. Az elektronikus iratkezelési szoftver akkor alkalmazható, ha megfelel a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről szóló jogszabály követelményeinek.

**A minősített adat nyilvántartási rendszere**

A minősített adat nyilvántartási rendszere alapvetően **két fő részre,** főnyilvántartásra és iratkezelési segédletekre osztható. A **főnyilvántartás alapja** a **főnyilvántartó könyv**, az **alapvető** iratkezelési segédletek pedig az iktatókönyv, a belső átadókönyv vagy más belső átadóokmány, valamint a külső kézbesítőkönyv vagy futárjegyzék.

**A főnyilvántartó könyv**

A minősített adatok kezeléséhez használatba vett hitelesített iratkezelési segédletek nyilvántartására szolgál a **főnyilvántartó könyv,** amely az iratkezelés elsődleges nyilvántartása. Minden szervnél **csak egy** van belőle, *nyilvántartásba nem kell venni*.

A főnyilvántartó könyvet a *titkos ügykezelés és a minősített adatok nyilvántartási rendszerének kialakításakor* a **minősített adatot kezelő szerv vezetője hitelesíti.** A minősített adatkezelő szerv *megszűnésekor* jegyzőkönyvvel kell**átadni a jogutód szervnek**. *Jogutód nélküli megszűnés esetén a* főnyilvántartó könyvet *az illetékes* **levéltár részére kell átadni**.

Rovatrendszere: sorszám, iratkezelési segédlet megnevezése, terjedelme, a használatbavételének és végleges lezárásának dátuma, az iratkezelési segédlet irattári tételszáma és kezelési bejegyzés.

**Iratkezelési segédletek**

**Iktatókönyv**

Aziktatókönyvben *kell nyilvántartásba* venni a minősített adatot kezelő szervhez **érkezett** vagy **ott keletkezett** minősített adathordozókat. Az iktatókönyvet a **főnyilvántartó könyvben** kell *(fő)nyilvántartásba venni* (pl.: 12. Fnyt). Munkaköri leírásban kapott felhatalmazás alapján az iktatókönyvet a **titkos ügykezelő** **hitelesíti**.

A pontos iktatás *biztosítja* az **adathordozók meglétét**, segítségével *nyomonkövethető* a **minősített adathordozó mozgása** és *elősegíti* a határidőket figyelembevevő **pontos ügyintézést**. Az iktatás során a minősített adathordozók az iktatókönyv **évente újrakezdett** *sorszámát* - alszámra történő iktatás során *alszámát* - kapják, az *évszám* egyidejű feltüntetésével és a szervezet által meghatározott *egyedi azonosítóval*. (pl.: 126/2010/B.; IV-NBF/3/8/2010.). **Az iktatókönyvet év végén le kell zárni és nem selejtezhető.**

**Belső átadókönyv vagy más belső átadóokmány**

A minősített adat *átadásának*, *továbbításának* és *visszavételének* igazolása, dokumentálása **nagy figyelmet** és még nagyobb **adminisztratív fegyelmet** igényel a minősített adathoz jogszerűen hozzáférő és *felhasználóvá* váló személyektől. Nemcsak a titkos ügykezelőktől, hanem valamennyi felhasználói jogosultsággal rendelkező vezetőtől, illetve beosztott munkatárstól egyaránt. Az átadás, visszavétel és a továbbítás szabályainak *normaszerű és következetes alkalmazása* nélkülözhetetlen ahhoz, hogy a minősített adatot kezelő szerveknél a minősített adathordozók útját, mozgását kétséget kizáró módon **nyomon lehessen követni**. A minősített adatok adminisztrációja során a **"zéró bizalom" elvét** kell alkalmazni, azaz a **minősített adathordozó teljes mozgását (valamennyi átadást, átvételt stb.) pontosan dokumentálni kell.** Ezt az elvet akkor is érvényesíteni kell, ha a minősített adat átadása *felettes vezető részére* történik! A titkos ügykezelőnek munkája során mindvégig, a tevékenység *valamennyi fázisában érvényesítenie kell* a **dokumentáltság elvét;** különösen figyelni kell erre a minősített adathordozó szerven belül történő átadásakor és visszavételekor Ez azt jelenti, hogy a minősített adathordozóval semmi sem történhet anélkül, hogy az a megfelelő nyilvántartásba bejegyzésre ne kerülne. Súlyos hibának számít és akár büntetőjogi következményei lehetnek annak, ha a minősített adathordozó átadása során az átadás tényét a titkos ügykezelő az átvevővel nem íratja alá.

Az átadásra, továbbításra és visszavételre meghatározott, a gyakorlati munka során sokszor bürokratikusnak, az ügyintézői munkát akadályozónak ítélt jogszabályi előírásoknak *a minősített adathordozók eltűnése* miatt időnként bekövetkező „**titoksértések” megelőzésében** is fontos szerepük van. A gyakorlati tapasztalatok azt mutatják, hogy azoknál a minősített adatkezelő szerveknél **magas** szintű a vezetőknek és a munkatársaknak az átvett **minősített adathordozókkal kapcsolatos felelősségérzete**, ahol az iratkezelési segédletek alapján **mindenki pontosan elszámoltatható** a jogszerűen *birtokába került minősített adathordozóval*. Ellenkező esetben, vagyis **felületes, laza adminisztráció esetén** a minősített adatokért érzett felelősség is alacsonyabb szintű és a minősített **adathordozó elvesztése, eltűnése** is nagyobb eséllyel következhet be.

A minősített adat **továbbítása** esetén a minősítő rendelkezése szerint kell eljárni. Amennyiben a minősített adathordozón a *továbbításra vonatkozóan* **külön rendelkezés nincs**, akkor azt kell *vélelmezni*, hogy a **minősítő** nem kívánta a minősített adatot a **címzetten kívül** *másnak* *továbbítani.* Ez esetben a **címzett a minősített adatot** a *vezetése, irányítása* alatt álló szerv **jogosultjain**, valamint az *állami feladat* végrehajtásában *közreműködőkön kívül* **másnak nem adhatja át**. Ha ezen kívül a minősített adat *más szerv vagy személy részére történő átadása* valamilyen **okból szükséges**, akkor ehhez az *átadás előtt* a **címzettnek meg kell kérnie** a minősítő **írásbeli engedélyét**, illetve **hozzájárulását**.

A minősített adat szerven belüli *átadása, visszavétele* csak a titkos ügykezelő útján, **belső átadókönyvben vagy más átadó okmányon**, sajátkezű, dátummal ellátott aláírás ellenében, dokumentáltan történhet. **Elektronikus iratkezelő szoftver** alkalmazása esetén minősített adatszerven belüli átadására, átvételére úgy kerülhet sor, hogy az elektronikus iratkezelő rendszer a *feleket hitelesítő szolgáltatás (PKI) vagy jelszavak segítségével* azonosítja, és az átadás-átvétel az elektronikus iratkezelő rendszerben rögzítésre kerül.

A minősített adathordozó **szerven belül** történő *átadására és visszavételére* szolgáló **iratkezelési segédletnek tartalmaznia kell:**

a) a minősített adat iktatószámát,

b) a minősítés szintjét,

c) a példánysorszámot,

d) a példányonkénti terjedelmet,

e) a címzettet,

f) az átadás dátumát,

g) az átadás tényének igazolását az átvevő nevének és saját kezű, dátummal ellátott aláírásának feltüntetésével,

h) a visszavétel dátumát,

i) a visszavétel tényének igazolását a visszavevő nevének és saját kezű, dátummal ellátott aláírásának feltüntetésével.

A minősített adathordozó szerven belüli átadásakor a titkos ügykezelő a belső átadókönyv vagy átadókarton következő sorszámán bejegyzi az átadásra kerülő minősített adathordozó azonosító adatait, majd az **átvevő** az átvételt *keltezéssel és olvasható aláírással igazolja.*

A dokumentáltság elvére való tekintettel a minősített adathordozó *átadásához* hasonlóan a *visszavétel* is csak a titkos ügykezelő útján, dokumentáltan, **belső átadókönyvben** vagy más belső **átadóokmányban** történhet. A *„zéró bizalom elve”* megköveteli, hogy a titkos ügykezelő *pontosan azonosítsa a visszavételre kerülő* minősített adathordozót, mielőtt annak visszavételét aláírásával igazolná. Meg kell győződnie a minősített adathordozónak a nyilvántartásban foglaltak szerinti **hiánytalan meglétéről** és arról, hogy **hányadik sorszámú példány** *visszavételét igazolja.*

**Külső kézbesítő könyv vagy futárjegyzék**

A minősített adatot tartalmazó küldeményt más szerv részére **zárt küldeményként,** a titkos ügykezelőn keresztül, kézbesítőkönyvben vagy futárjegyzéken dokumentálva kell továbbítani. A továbbítás tényét a titkos ügykezelőnek az iktatókönyvben is rögzítenie kell.

Minősített küldemény:

- *belföldre* csak a)az **Állami Futárszolgálat**,

 b) a Magyar Honvédség Katonai Futárszolgálata

c) a katonai futár és a rendvédelmi szervek belső futára, valamint

d) sürgős esetben kivételesen személyes kézbesítő útján,

-*külföldre* a **Külügyminisztérium** útján továbbítható.

**Minősített küldeményt postai úton, „civil” futár- vagy csomagküldő szolgálattal továbbítani tilos!**

Nemzeti minősített adatot tartalmazó küldemény **borítékján, csomagolásán** a címzett és a feladó adatain kívül fel kell tüntetni minősített adat iktatószámát, minősítési szintjét, példánysorszámát és „Baleset esetén vagy rendkívüli helyzetben a küldő szerv bonthatja fel!” figyelmeztetést, valamint a különleges kezelési utasítást. Állami Futárszolgálattal való továbbítás esetén fel kell tüntetni a küldő szerv futárkódszámát is. A küldemény úgy kell lezárni, hogy az esetleges felbontás, jogosulatlan hozzáférés ténye egyértelműen megállapítható legyen.

**A minősített adatot tartalmazó adathordozó irattározása és a megsemmi-sítési eljárás**

Az NBF kormányrendelet szerint a **minősítés megszüntetése vagy megszűnése előtt** a **saját készítésű** minősített adatot tartalmazó adathordozó **eredeti irattári példánya** - amennyiben törvény másként nem rendelkezik - **nem selejtezhető és nem semmisíthető meg**.

A más szervtől kapott, valamint a saját készítésű minősített adatot tartalmazó adathordozó, **ügyviteli érdeket nem képviselő többes példánysorszámú** **példányai** a minősített adatot kezelő szerv vezetője vagy általa adott felhatalmazás alapján a biztonsági vezető jóváhagyását követően **megsemmisíthetők**.

A megsemmisítésről minden esetben **megsemmisítési jegyzőkönyvet** kell készíteni. A jegyzőkönyvnek tartalmaznia kell a megsemmisítésre kerülő többes példánysorszámú adathordozón szereplő minősített adatok azonosításához szükséges adatokat (iktatószám, minősítési szint, terjedelem, példánysorszám), valamint a megsemmisítés tényét, módját és dátumát, a megsemmisítésnél jelen lévők és a megsemmisítést engedélyező vezető aláírását.

A megsemmisítés a titkos ügykezelő, valamint a biztonsági vezető által a minősített adatot kezelő szerv állományából kijelölt, a megsemmisítendő adathordozón szereplő minősített adatra érvényes felhasználói engedéllyel és személyi biztonsági tanúsítvánnyal rendelkező személyek jelenlétében történhet. A **megsemmisítést úgy kell végrehajtani**, hogy a megsemmisített adathordozón szereplő minősített adat **tartalmát utólag ne lehessen megállapítani.** A megsemmisítés **időpontját** és a megsemmisítési **jegyzőkönyv iktatószámát** az **iktatókönyvben rögzíteni** kell.

**Az elektronikus biztonság**

Az elektronikus biztonság részletes végrehajtási szabályait a Mavtv. felhatalmazása alapján kiadott, a minősített adat az elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V.6.) Korm. rendelet (Elektronikus kormányrendelet) állapítja meg

Az **Elektronikus kormányrendelet** a NATO és az EU biztonsági szabályzatainak előírásait szem előtt tartva, **a minimális követelményeket állapítja meg**, kellő rugalmasságot biztosítva ahhoz, hogy a minősített adat, valamint a minősített adatot kezelő rendszer védelme **a konkrét veszélyeztetettséghez igazodva, a költséghatékonyság figyelembevételével** biztosítsa a szükséges és elégséges védelem szintjét. Az elektronikus biztonság integrált részeként szabályozza a rejtjeltevékenységet, de a nemzetközi gyakorlatnak megfelelően e szakterület viszonylagos önállóságát megőrizve.

Az Elektronikus kormányrendelet részletesen meghatározza **az elektronikus biztonság helyi szervezeti és személyi elemeit** és azok feladatkörét, melyről a fentiekben részletesen írtunk. Az elektronikus biztonsági rendszerben a **Nemzeti Biztonsági Felügyelet** látja el az elektronikus biztonság tekintetében **a nemzeti engedélyező, a kommunikációbiztonsági és a kompromittáló kisugárzás biztonsági (TEMPEST) hatóság** feladatait.

Az Elektronikus kormányrendelet meghatározza a **rendszerbiztonság, a kommunikációbiztonság és a kompromittáló kisugárzás elleni védelem követelményrendszerét**, valamint az **engedélyezési** és **ellenőrzési** eljárás rendjét is.

A **rendszerbiztonság** keretében szabályozza a *hardverbiztonság,* a *szoftverbiztonság* követelményeit, a hozzáférési jogosultságokat, a *biztonsági mentés és helyreállítás*, a *vírusvédelem rendjét*, valamint meghatározza a rendszeren alkalmazható *biztonsági üzemmódokat* és a *hálózat biztonságára* vonatkozó intézkedéseket.

A **kommunikációbiztonság** tárgykörében alapvetően a rejtjelbiztonság korábbi szabályait vette át és ezen belül **egységes keretbe foglalta a nemzeti, a NATO és az EU rejtjeltevékenységre** vonatkozó követelményeket és eljárási rendet. Meghatározza azokat a kivételes körülményeket, amikor a minősített adat rejtjelzés nélkül is továbbítható.

A **kompromittáló kisugárzás** biztonsági követelményrendszere vonatkozásában a NATO és EU irányelveket érvényesíti a nemzeti minősített adat védelmére is. Tekintettel arra, hogy a NATO és az EU irányelvek minősített adatot képeznek, így ezeket a követelményeket maga a jogszabály nem részletezi, de kimondja, hogy a konkrét rendszerre vonatkozó követelményeket az NBF ezen irányelvek alapján állapítja meg. A követelmények minősítését az indokolja, hogy azok nyilvánossá tétele megkönnyítené a rendszer támadását.

Az Elektronikus kormányrendelet részletesen szabályozza az **engedélyezési eljárást**. Az engedélyezési eljárás során **a hatósági jogkört első fokon** a **Nemzeti Biztonsági Felügyelet** gyakorolja. A minősített adatot elektronikusan kezelő rendszert üzemeltető valamennyi szervnek rendelkeznie kell az NBF által kiadott **rendszerengedéllyel.** Szükség szerint – illetve „Szigorúan titkos!” minősítési szintű adatok esetén kötelező jelleggel – a Nemzeti Biztonsági Felügyelet **helyszíni szemlét** tart és meghatározza a rendszer kialakításához szükséges intézkedéseket annak érdekében, hogy a felesleges beruházások elkerülhetők legyenek.

Az elektronikus biztonság, ezen belül a rejtjelbiztonság **veszélyeztetése esetén** a **Nemzeti Biztonsági Felügyelet** a rendszer használatát **korlátozhatja, megtilthatja**, a szerv vezetőjét a rendszerbiztonság helyreállítása érdekében szükséges **intézkedésekre kötelezheti** és a kiadott engedélyeket **visszavonhatja.**

**A kompromittáló elektromágneses kisugárzás elleni védelem (TEMPEST)**

A Nemzeti Biztonsági Felügyelet feladatainak része az elektronikus eszközök kompromittáló elektromágneses kisugárzása elleni védelem. Minden elektronikus eszköz bocsát ki ugyanis magából elektromágneses jeleket. A technika fejlődése lehetővé tette, hogy az elektronikus eszközök által **kibocsátott** elektromágneses **jelekből visszaállítható** legyen az adott eszközön kezelt **minősített adat**. Az ezzel szembeni védekezés egyik alapvető eszköze az ilyen kompromittáló kisugárzás minimális szintre csökkentése, ami megakadályozza a minősített információk illetéktelen kezekbe jutását. E módszer szabályait a NATO-ban és az EU-ban egyaránt az úgynevezett TEMPEST összefoglaló név alatt tárgyalják.

**A minősített adat megismerése**

A Mavtv. megteremtette az elvi lehetőségét annak, hogy **bárki** **megismerhesse nemzeti minősítésű saját személyes adatát**, amennyiben számára ezt a kért adat minősítője megismerési engedély kiadásával engedélyezi. A **megismerési kérelmet csak a minősítő** jogosult elbírálni, mert kizárólag ő rendelkezik a minősítés indokoltságát megalapozó információkkal. A megismerési kérelemre nézve nincs formakényszer, elegendő a kért minősített adat megjelölése. A megismerési engedély kiadásáról az érintett kérelmére a minősítő **15 napon belül köteles határozni**.

A megismerési engedély kiadását követően, annak alapján, a kérelmező személyi biztonsági tanúsítvány – és az ehhez szükséges nemzetbiztonsági ellenőrzés nélkül – jogosult nemzeti minősítésű személyes adatának megismerésére. A kérelmező köteles a nemzeti minősített adat megismerése előtt írásban **titoktartási nyilatkozatot** tenni és a nemzeti minősített adat védelmére vonatkozó szabályokat betartani.

A megismerési engedély kiadását a minősítő **köteles megtagadni**, ha az adat megismerése a minősítés alapjául szolgáló **közérdek sérelméhez vezet**. A megismerési engedély megtagadását a minősítőnek **indokolnia kell**. A megismerési engedély megtagadása esetén az érintett a határozat kézhezvételét követő **15 napon belül a Fővárosi Bírósághoz fordulhat**. Ha a bíróság a **kérelemnek helyt ad**, a minősítőt **a megismerési engedély kiadására kötelezi**. A bíróság eljárására a polgári perrendtartás közigazgatási perekre vonatkozó rendelkezéseit kell alkalmazni azzal, hogy a bíróság az ügyben zárt tárgyaláson, soron kívül jár el. A perben csak olyan bíró járhat el, akinek a nemzetbiztonsági szolgálatokról szóló törvény szerinti legmagasabb szintű nemzetbiztonsági ellenőrzését elvégezték. A **felperes**, a felperes oldalán beavatkozó személy és ezek képviselője a minősített adatot **az eljárás során nem ismerheti meg**. A perben résztvevő egyéb személyek, valamint azok képviselői a minősített adatot csak akkor ismerhetik meg, ha a nemzetbiztonsági szolgálatokról szóló törvény szerinti legmagasabb szintű nemzetbiztonsági ellenőrzésüket elvégezték.

A minősített adat kezelője a személyes adatok védelméről szóló törvény alapján az érintettet megillető **tájékoztatást megtagadhatja**, ha a minősítés alapjául szolgáló **közérdeket** az érintettnek a személyes adatainak kezelésére vonatkozó tájékoztatása **veszélyeztetné**.

**A minősített adat felhasználása**

**Általános szabályok**

Főszabályként elmondható, hogy minősített adatot csak az a személy használhat fel, akinek ez állami vagy közfeladat ellátása érdekében indokolt, és aki – törvényben meghatározott kivételektől eltekintve – rendelkezik

* érvényes és a felhasználni kívánt adat minősítési szintjének megfelelő személyi biztonsági tanúsítvánnyal,
* titoktartási nyilatkozattal, valamint
* felhasználói engedéllyel.

A **„Korlátozott terjesztésű!”** minősítési szintű minősített adat állami vagy közfeladat ellátásához szükséges felhasználása esetén a felhasználónak személyi biztonsági tanúsítvánnyal nem, csak felhasználói engedéllyel kell rendelkeznie és titoktartási nyilatkozatot kell tennie.

A minősített adat felhasználásának számos, a főszabálytól eltérő esetét határozza meg a Mavtv.

**A nemzetbiztonsági ellenőrzés**

A nemzetbiztonsági ellenőrzés szabályait a nemzetbiztonsági szolgálatokról szóló **1995. évi CXXV. törvény** határozza meg.

A nemzetbiztonsági szolgálatok által végzett nemzetbiztonsági ellenőrzés célja annak vizsgálata, hogy fontos és bizalmas munkakörre jelölt, illetve az ilyen munkakört betöltő személyek megfelelnek-e az állami élet és a nemzetgazdaság jogszerű működéséhez elengedhetetlen, valamint - amennyiben szükséges - a nemzetközi kötelezettségvállalásokból fakadó biztonsági feltételeknek.

Az ellenőrzést a kezdeményezésre jogosult saját mérlegelési jogkörében - de **legalább ötévenként** - kezdeményezi.

Az érintett személyt előre tájékoztatni kell a biztonsági ellenőrzés elrendelésének lehetőségéről és annak lehetséges módjairól, ugyanis az ellenőrzés csak az előzetes írásbeli hozzájárulásával folytatható le.

Ha az érintett személy az ellenőrzéshez nem járul hozzá, fontos és bizalmas munkakörben nem foglalkoztatható.

„Korlátozott terjesztésű!” minősítési szintű adat felhasználásához nincsen szükség nemzetbiztonsági ellenőrzésre.

**A személyi biztonsági tanúsítvány**

A személyi biztonsági tanúsítvány igazolja, hogy az elvégzett nemzetbiztonsági ellenőrzés alapján a minősített adatot felhasználó személy meddig és milyen minősítési szintű adatokhoz férhet hozzá.

A minősített adatot kezelő szervezet – a gazdálkodó szervezet kivételével – **biztonsági vezetője**

* adja ki a szerven belül – a Nemzeti Biztonsági Felügyelet honlapján közzétett minta alapján egy példányban – a nemzeti minősített adatra érvényes személyi biztonsági tanúsítványát a nemzeti minősített adatot felhasználók, valamint a szervvel közreműködők részére,
* a szükséges biztonsági feltételek hiánya vagy megszűnése esetén a személyi biztonsági tanúsítvány kiállítását megtagadja, illetve a már kiadott tanúsítványt visszavonja.

A nemzeti minősített adatra érvényes személyi biztonsági tanúsítvány tartalmazza:

* a személyi biztonsági tanúsítványt kiadó minősített adatot kezelő szerv megnevezését,
* az érintett személy természetes személyazonosító adatait,
* a kiadott személyi biztonsági tanúsítvány nyilvántartási számát, keltét, érvényességi idejét és a felhasználó által felhasználható nemzeti minősített adat legmagasabb minősítési szintjét,
* a személyi biztonsági tanúsítvány kiadására jogosult vezető aláírását.

A nemzeti minősített adatra érvényes személyi biztonsági tanúsítvány kezelését és tárolását a biztonsági vezető vagy az e feladattal általa írásban kijelölt személy vagy szerv végzi.

A nemzeti minősített adatra érvényes személyi biztonsági tanúsítvány visszavonását követően a biztonsági vezető intézkedik a személyi biztonsági tanúsítvány selejtezéséről.

A biztonsági vezető gondoskodik arról, hogy a titkos ügykezelő naprakész és pontos információval rendelkezzen a minősített adatot kezelő szervnél érvényes személyi biztonsági tanúsítvánnyal rendelkező személyekről.

**A Nemzeti Biztonsági Felügyelet adja ki**

* a külföldi minősített adat felhasználói, továbbá
* a minősített adatot kezelő gazdálkodó szervezetek felhasználói részére a személyi biztonsági tanúsítványt.

Mindkét esetben a kezdeményezés a kérelmező

* vezetéknevét, utónevét,
* születési helyét, születési idejét,
* állampolgárságát,
* a munkáltatójának és a munkakörének megnevezését és
* a megismerni kívánt adatfajta minősítési szintjét tartalmazó

a Nemzeti Biztonsági Felügyelet honlapján közzétett adatlap kitöltésével történik.

**A felhasználói engedély és a titoktartási nyilatkozat**

Felhasználó az a személy, akinek állami vagy közfeladat végrehajtása céljából a felhasználói engedély kiadására jogosult vezető a minősített adatra vonatkozóan a felhasználói engedélyben rendelkezési jogosultságokat biztosít;

A **felhasználói engedély** mindig **visszavonásig érvényes**, mert ez a jog általában meghatározott beosztáshoz, munkakörökhöz kapcsolódik. A felhasználó azonban ezt a jogát másra nem ruházhatja át. A felhasználói engedély kiadására általában a kinevezéssel, illetve a megbízással egyidejűleg kerül sor. Ez természetesen nem zárja ki, hogy a munkavégzéssel összefüggő jogviszony keletkezésétől időben elváljon. A jogviszony megszűnésével viszont e jogosítvány is visszavonásra kerül.

A felhasználói engedélyben meg kell határozni, hogy a rendelkezési jogosultságok közül melyek illetik meg a felhasználót.

A minősített adatra vonatkozó rendelkezési jogosultságok:

* állami vagy közfeladat végrehajtása érdekében történő ügyintézés, feldolgozás,
* minősített adat nyilvántartásával kapcsolatos valamennyi tevékenység,
* minősített adat birtokban tartása,
* minősítési jelölés megismétlése, illetve a megismétlés megtiltása,
* minősített adat másolása, sokszorosítása,
* minősített adat fordítása,
* kivonat készítése,
* szerven belüli átadás,
* szerven kívülre továbbítás, szállítás,
* selejtezés, illetve megsemmisítés,
* felhasználói engedély kiadása,
* megismerési engedély kiadása,
* nemzeti minősített adat felülvizsgálata,
* minősített adat külföldi személy vagy külföldi szerv részére hozzáférhetővé tételének engedélyezése,
* minősített adat külföldre vitelének vagy külföldről való behozatalának engedélyezése,
* titoktartási kötelezettség alóli felmentés.

A felhasználót

* a saját minősítésű adat esetén a rendelkezési jogosultságok teljes körűen illetik meg,
* a más minősítő által minősített adat esetén az *a)-k)* pontokban foglalt rendelkezési jogosultságok

illethetik meg.

A biztonsági vezető felelőssége, hogy az a felhasználó, akinek a feladata ellátásához ez szükséges – a meghatározott kivételekkel –, felhasználói engedéllyel és általa aláírt titoktartási nyilatkozattal rendelkezzen.

Egyazon felhasználói engedélyben nemzeti és külföldi minősített adat felhasználására is adható felhatalmazás, ennek megfelelően a felhasználói engedélyben meghatározott minősített adatok meghivatkozásával elegendő egy titoktartási nyilatkozatot aláírni.

A felhasználói engedély és a titoktartási nyilatkozat kezeléséről, valamint tárolásáról a biztonsági vezető a minősített adatkezelő szerv Biztonsági szabályzatában meghatározottak szerint intézkedik.

A szignálásra jogosult vezető felelőssége, hogy olyan felhasználó részére engedélyezze a minősített adat felhasználását, aki – meghatározott kivételekkel – rendelkezik felhasználói engedéllyel és általa aláírt titoktartási nyilatkozattal.

A minősített adat felhasználására való jogosultság a felhasználói engedély visszavonásával szűnik meg.

A felhasználói engedélyt a kiadására jogosult vezető visszavonja, ha a felhasználó

* munkaviszonya, köztisztviselői, közalkalmazotti, bírói, igazságügyi, ügyészi, hivatásos szolgálati jogviszonya vagy a hivatásos és szerződéses katonák jogállásáról szóló törvény szerinti szolgálati viszonya megszűnik vagy
* feladata ellátásához a továbbiakban minősített adat felhasználása nem szükséges, valamint ha
* személyi biztonsági tanúsítványa visszavonásra került vagy érvényessége lejárt.

A biztonsági vezető felelőssége, hogy a minősített adatot kezelő szervnél tárolt felhasználói engedély és titoktartási nyilatkozat a felhasználói engedély visszavonását követően a visszaélés szigorúan titkos és titkos minősítésű adattal bűncselekményre a büntető törvénykönyvben meghatározott büntetési tétel felső határának megfelelő ideig fellelhető legyen. Ezt követően intézkedik ezen okmányok selejtezési jegyzőkönyv felvétele mellett történő megsemmisítéséről.

**Minősített adat átadása közreműködő részére**

A **közreműködő olyan természetes személy**, aki az állami vagy közfeladatot ellátó szerv feladat- és hatáskörébe tartozó ügyben segítséget nyújt, és ehhez minősített adat felhasználása is szükséges.

Ha a minősített adatot kezelő szerv közreműködő segítségét veszi igénybe, és ehhez a közreműködőnek minősített adatot kell felhasználnia, - a minősítő eltérő rendelkezésének hiányában - a közreműködő részére a minősített adatot kezelő szerv vezetője adja ki a felhasználói engedélyt.

A felhasználói engedély megadása előtt a minősített adatot kezelő szerv köteles ellenőrizni, hogy a közreműködőnél megteremtették-e a minősített adat védelméhez előírt feltételeket, vagyis ellenőriznie kell a személyi, a fizikai, az adminisztratív és az elektronikus biztonságra vonatkozó feltételek meglétét.

A közreműködőre az őt igénybe vevő minősített adatot kezelő szerv részére meghatározott személyi, fizikai, adminisztratív és elektronikus biztonságra vonatkozó feltételek vonatkoznak.

A **felhasználói engedély nem adható ki**, ha a közreműködő **nem felel meg a személyi biztonsági feltételeknek**, így például nem rendelkezik vagy nem adható ki részére megfelelő szintű személyi biztonsági tanúsítvány.

A közreműködő kizárólag a minősített adatot kezelő szervnél férhet hozzá a minősített adathoz, ha a minősített adatot kezelő szerv az ellenőrzése során megállapítja, hogy a közreműködőnél hiányoznak

* a fizikai biztonságra,
* az adminisztratív biztonságra vagy
* az elektronikus biztonságra

vonatkozó feltételek, de a személyi biztonsági feltételeknek megfelel.

**Büntetőjogi és szabálysértési szankciók**

**A Büntető Törvénykönyv módosítása**

A Büntető Törvénykönyv Mavtv. általi módosítása az egyes minősítési szintekhez igazodóan tovább differenciálta a büntetőjogi szankciórendszert. Az „államtitok és a szolgálati titok megsértése” bűncselekmények helyébe a **„visszaélés szigorúan titkos és titkos minősítésű adattal”**, a **„visszaélés bizalmas minősítésű adattal”**, valamint a **„visszaélés korlátozott terjesztésű minősítésű adattal”** bűncselekmények léptek. A szankciórendszer ily módon történő differenciálása a hatékonyabb büntetőjogi védelmet hivatott biztosítani. A Btk. államtitok és szolgálati titok megsértésére vonatkozó tényállásai ugyanis nem álltak összhangban a NATO szabályozásával sem. Példának okáért, azt az elkövetőt, aki több tucat „NATO Titkos!” minősítésű adattal élt vissza, csupán szolgálati titoksértés bűncselekménye miatt lehetett felelősségre vonni.

További változást jelent, hogy a **gondatlan elkövetést** csak a minősített adat felhasználására törvény rendelkezése alapján jogosult személy esetében rendeli büntetni a törvény, tehát „civil személynél” kizárólag a szándékos elkövetést szankcionálja a Btk. A tekintetben is különbséget tesz a törvény a minősített adat felhasználására törvény rendelkezése alapján jogosult személy általi elkövetés, illetve a „civil személy” általi elkövetés között, hogy amennyiben a bűncselekmény alanya minősített adat védelmére kötelezett személy, azt súlyosabban rendeli büntetni. Súlyosbító körülményt jelent, ha a minősített adat jogosulatlan külföldi személy részére válik hozzáférhetővé.

**Szabálysértési szankciók**

A minősített adatok kezelésére vonatkozó szabályok megsértése esetén a szankciós védelmet a **szabálysértési jog** és **a büntetőjog** biztosítja. Az általuk nyújtott védelemnek a két jogág természetéből adódóan a legutolsó eszköznek (ultima ratio) kell lennie a jogtárgy védelme során. Az egyes szabálysértésekről szóló 218/1999. (XII.28.) Korm. rendelet 25.§-a a ***„Minősített adat biztonsága megsértése”*** néven foglalja össze azokat a jogellenes magatartásokat, amelyek a bűncselekményhez képest enyhébb mértékben sértik vagy veszélyeztetik a minősített adatok kezelésének rendjét. Általános jogelv, hogy nem állapítható meg szabálysértés, amennyiben az elkövetett cselekmény bűncselekményt valósít meg. A *„Minősített adat biztonsága megsértése”* szabálysértés elkövetése esetén az eljárás lefolytatása a **rendőrség** hatáskörébe tartozik.

**A büntetőeljárás egyes rendelkezései**

A büntetőeljárásról szóló 1998. évi XIX. törvény alapján a büntetőjogi felelősségre vonás ok-okozati összefüggésének elemei a következők:

* az adat védelméhez fűződő érdek felismerése;
* a minősített adat védelméről szóló törvény szerinti minőségében meghatározott személy, igazolható közérdekvédelmi célból szabályozott eljárás lefolytatása;
* fenti eljárás eredményeként létrejövő minősítéssel védett adat;
* a minősítés alapjául szolgáló védelmi érdek sérelme és az azt kiváltó cselekmény közötti összefüggés bizonyítása;
* **büntetőeljárás lefolytatása**;
* büntetés kiszabása.

A bíróság tárgyalása nyilvános. A bíróság hivatalból vagy az érdekeltek indítványára a nyilvánosságot az egész tárgyalásról vagy annak egy részéről határozattal kizárhatja, és zárt tárgyalást rendelhet el, haazt a minősített adat védelme indokolja. A büntetőeljárás során a nyilvánosság tájékoztatását és a sajtó felvilágosítását meg kell tagadni, ha az a minősített adat védelmét sértené, vagy egyébként az eljárás eredményes lefolytatását veszélyeztetné. A tanúkra vonatkozó szabályoknál a törvény kimondja, hogy minősített adatról nem hallgatható ki tanúként az, aki a titoktartási kötelezettség alól nem kapott felmentést.