NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

KÖZIGAZGATÁSI TOVÁBBKÉPZÉSI INTÉZET

TÁJÉKOZTATÓ

az ügykezelői alapvizsga

tananyagát érintő változásokról

Budapest, 2025. március 10.

Tisztelt Vizsgázó!

A Nemzeti Közszolgálati Egyetem (a továbbiakban: NKE) jogszabályban rögzített feladata, hogy az ügykezelői alapvizsgához kapcsolódó ismeretanyagot időközönként hatályosítsa. A közigazgatási és az ügykezelői alapvizsgáról szóló 174/2011. (VIII. 31.) Korm. rendelet 3. § (3) bekezdése kimondja, hogy az NKE feladata az ügykezelői alapvizsga követelményrendszerének, országosan egységes oktatási programjának, tananyagának és a követelményrendszeren alapuló vizsgatételeinek kifejlesztése, valamint szükség szerint – különösen, amennyiben a jogszabályi változások indokolják – aktualizálása.

A jogszabályi kötelezettségen alapuló hatályosítást, a tananyag átdolgozását a Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézete (a továbbiakban: NKE KTI) a 2025. január 01-jéig kihirdetett jogszabályok alapján zárta le. Az NKE KTI fontosnak tartja, hogy a tisztviselők ismereteiket a hatályosított tananyag alapján sajátítsák el, és a 2025. tavaszi vizsgaidőszak folyamán már a tankönyv lezárása, korábbi hatályosítása óta bekövetkezett jogszabályi módosulások is megjelenjenek a tananyagban, s egyben a számonkérés alapját is képezzék.

A tananyag-kiegészítő dokumentumban minden jelentősebb, az adott fejezetcímen belül végrehajtott módosítást az oldalszám és a bekezdés feltüntetésével, vastagon kiemelve jelöltünk. Az új, hatályos szövegrészeket pirossal szedtük, míg a hatályát vesztett részek fekete áthúzással szerepelnek. Az egyes módosítások indoklásait dőlt betűvel, az adott módosított szövegrészt követően rögzítettük.

A tananyag-kiegészítő dokumentum kibocsátásával az NKE KTI segítséget kíván nyújtani, hogy az ügykezelői alapvizsgára Ön a lehető legnaprakészebben tudjon felkészülni.

Eredményes felkészülést és sikeres vizsgát kívánunk!

Budapest, 2025. március 10.

Nemzeti Közszolgálati Egyetem
Közigazgatási Továbbképzési Intézet

I. FEJEZET: A közigazgatás felépítése és működése

2.1. A KÖZPONTI ÁLLAMIGAZGATÁSI SZERVEK

A 10. oldal szövege az alábbiak szerint módosul:

1. a Kormány;
2. a minisztériumok;
3. a kormányzati főhivatalok;
4. a központi hivatalok;
5. az autonóm államigazgatási szervek;
6. az önálló szabályozó szervek;
7. ~~rendvédelmi szervek és a Katonai Nemzetbiztonsági Szolgálat.~~

7 a rendvédelmi szervek

8. a nemzetbiztonsági szolgálatok

Indokolás: a 2010. évi XLIII. törvény 1.§-a módosult.

2.1.4. A nem minisztériumi formában működő központi közigazgatási szervek csoportjai

A 14. oldal szövege az alábbiak szerint módosul:

5. a rendvédelmi szervek és a nemzetbiztonsági szolgálatok ~~Katonai Nemzetbiztonsági Szolgálat~~ (a rendőrség, büntetés-végrehajtási szervezet, hivatásos katasztrófavédelmi szerv, polgári nemzetbiztonsági szolgálat, Katonai Nemzetbiztonsági Szolgálat).

Indokolás: a 2010. évi XLIII. törvény 1.§-a módosult.

A 15. oldal szövege az alábbiak szerint módosul:

A rendvédelmi szervek és a nemzetbiztonsági szolgálatok ~~a Katonai Nemzetbiztonsági Szolgálat~~ speciális feladataik és jogállásuk miatt kerültek külön kategóriába. A rendvédelmi szervek és a nemzetbiztonsági szolgálatok a nem civil közigazgatáshoz tartozó szerveket jelentik. Tevékenységük elsősorban a társadalmi béke megőrzésére, az állam külső és belső védelmének biztosítására, a társadalomellenes cselekvések megelőzésére, üldözésére irányul. Jellemző rájuk, hogy tagjaik egyenruha-viselésre kötelezettek, fegyverviselésre jogosultak.

Indokolás: a 2010. évi XLIII. törvény 1.§-a módosult.

II. FEJEZET: A közszolgálati tisztviselők jogviszonya

2. A KÖZSZOLGÁLATI TISZTVISELŐKRE VONATKOZÓ JOGI SZABÁLYOZÁS
A 30. oldalon a szöveg az alábbiak szerint módosul:

A törvény a központi kormányzati igazgatási szervek kormánytisztviselőinek rendelkezéseit írja le részletesen, és a többi személyi körrel kapcsolatban csak az ettől eltérő szabályokat tartalmazza. A Kttv. ezzel szemben elsősorban a helyi önkormányzatok képviselő-testületének hivatalaiban (polgármesteri hivatalban vagy közös önkormányzati hivatalban) dolgozó köztisztviselők és közszolgálati ügykezelők jogviszonyát szabályozza. ~~(eltekintve a szűk körben foglalkoztatott kormánytisztviselőkre és kormányzati ügykezelőkre vonatkozó főszabályoktól).~~

Indokolás: jogszabályi változások miatt a szöveg módosítása.

3.4. AZ ÜGYKEZELŐKRE VONATKOZÓ ELTÉRŐ RENDELKEZÉSEK
A 35. oldalon a szöveg az alábbiak szerint módosul:

~~A Kttv.-nek a kormányzati ügykezelőkre (lásd VI. Fejezet) vonatkozó fejezete csak azokat a rendelkezéseket tartalmazza,~~ ~~**amelyek eltérnek a Kttv. kormánytisztviselőkre vonatkozó szabályaitól,**~~ ~~minden más esetben rájuk is ugyanazok a szabályok vonatkoznak, mint a kormánytisztviselőkre. A közszolgálati ügykezelők jogviszonyára a kormányzati ügykezelőkre vonatkozó rendelkezéseket nem lehet alkalmazni. Ugyanez az analógia alkalmazható a köztisztviselők és a közszolgálati ügykezelők viszonyában is.~~

A közszolgálati ügykezelő közszolgálati jogviszonyában a köztisztviselőkre vonatkozó meghatározott rendelkezéseket eltérésekkel, megfelelően kell alkalmazni.

Indokolás: egyszerűsítés, pontosítás.

III. FEJEZET: A közigazgatási hatósági eljárás szabályai

3.2. ELSŐFOKÚ ELJÁRÁS

A 43. oldal negyedik bekezdésének szövege az alábbiak szerint módosul:

Automatikus döntéshozatali eljárásnak akkor van helye, ha a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény (Dáptv.) ~~az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (Eüsztv.)~~ szerinti automatikus döntéshozatali eljárás feltételei fennállnak és nincs ellenérdekű ügyfél, vagy a kérelem tekintetében azt törvény vagy kormányrendelet megengedi, a hatóság részére annak benyújtásakor minden adat rendelkezésére áll, a döntés meghozatala mérlegelést nem igényel, és nincs ellenérdekű ügyfél.

Indokolás: az Ákr. módosítása és az Eüsztv. hatályon kívül helyezése (2024. évi XII. törvény).

IV. FEJEZET: A KÖZIGAZGATÁS INFORMATIKAI TÁMOGATÁSA

2.5.1 Elektronikus rendszerek biztonsága

A 65. oldal utolsó bekezdésének szövege az alábbiak szerint módosul:

Az informatikai és egyéb elektronikus rendszereket egyre több veszély fenyegeti. Mindennaposak manapság a kiber-bűnözésről (cybercrime), kiber-terrorizmusról (cyberterrorism) szóló tudósítások, melyek saját rendszereinket is fenyegetik. A rendszerek egységes kiberbiztonsági feltételeinek kialakítására ~~2013. áprilisában elfogadták~~ elfogadásra került a Magyarország kiberbiztonságáról szóló 2024. évi LXIX törvény. ~~az állami és önkormányzati szervek elektronikus biztonságáról szóló 2013. évi L. törvényt~~. A törvény hatálya a központi államigazgatási szerveken túl a helyi és vármegyei önkormányzatokra, a bíróságokra, az ügyészségekre, a honvédségre, a Nemzeti Bankra, ~~valamint~~ a közvetlenül az állam irányítási jogkörébe tartozó önálló szervekre, többségi állami befolyás alatt álló szervekre, kiemelten kockázatos és kockázatos ágazatokban működő szervezetekre, valamint a kritikus szervezetekre és infrastruktúrákra is kiterjed

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.1 Elektronikus rendszerek biztonsága

A 66. oldal első bekezdés szövege törlésre kerül:

~~A törvény jelentősége az, hogy hivatalosan is deklarálásra került, hogy az állami szervek által kezelt elektronikus rendszerek nemzeti adatvagyont alkotnak, amelynek védelme rendkívül összetett feladat~~

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.2 Az adatok osztályba sorolása, kapcsolódó tevékenységek és szabályok

A 66. oldal szövege az alábbiak szerint változik:

A törvény értelmében az annak hatálya alá tartozó szervezetek esetében az elektronikus információs rendszerek sértetlensége és rendelkezésre állásása, illetve az azokban tárolt adatok és szolgáltatások bizalmassága, sértetlensége és rendelkezésre állása tekintetében folyamatosan biztosítani kell a zárt, teljes körű és a kockázatokkal arányos védelmet. A megfelelő védelem érdekében ez érintett szervezetek esetében az alábbi feladatok elvégzése szükséges:

- kockázatmenedzsment keretrendszert kell létre hozni és működtetni,
- gondoskodni kell a szervezet általl használt elektronikus információs rendszerek felméréséről és nyilvántartásba vételéről
- fel kell mérni, és osztályozni kell a rendszerben kezelt adatokat
- biztonsági osztályba kell sorolni az elektronikus információs rendszereket
- meg kell határozni a rendszerek kapcsán szükséges védelmi intézkedéseket és biztosítani kell azok működését, illetve gondoskodni kell azok időszakos felülvizsgálatáról, szükség esetén módosításáról,
- információbiztonsági szabályzatot kell kiadni a szervezet vonatkozásában, és azt rendszeres időközönként felül kell vizsgálni
- gondoskodni kell a kiberbiztonsági hatósági kötelezések teljesítéséről.

Fenti feladatokat a szervezet vezetője az elektronikus információs rendszer biztonságáért felelő személy bevonásával, illetve a megfelelő szerepkörök kialakításával, a felelősségek megállapításával teljesíti.

A szervezet elektronikus információs rendszereit a kockázatokkal arányos védelem érdekében biztonsági osztályokba kell sorolni.

~~elektronikus információs rendszereit és az azokban található adatokat – bizalmasság, sértetlenség és rendelkezésre állás alapján –, valamint az azokat fejlesztő, az üzemeltetést végző, az üzemeltetésért felelős, illetve az információ biztonságért felelős szervezeti egységeket az információs rendszerek védelmére való felkészültségük alapján biztonsági osztályokba kell sorolni. A biztonsági osztályba sorolás során egytől ötig sorszámozott fokozatokat kell használni. Ha egy rendszer első biztonsági osztályba sorolt, akkor annak működtetéséhez alkalmazott előírások sokkal enyhébbek, mint a negyedik szint esetében. Minél magasabb a biztonsági osztály sorszáma, az abban tárolt adatok védelme során annál szigorúbb biztonsági intézkedéseket kell alkalmazni. A biztonsági osztályba sorolást háromévente, vagy szükség esetén soron kívül dokumentált módon felül kell vizsgálni. Soron kívüli felülvizsgálat szükséges jogszabályváltozás, új elektronikus információs rendszer bevezetése, vagy a szervezet által kezelt adatok körében bekövetkezett változás esetén..~~
~~A törvény hatálya alá tartozó szervezetek esetében a szervezetet is biztonsági osztályba kell sorolni.~~
~~Az egyes biztonsági osztályokhoz tartozó követelményrendszert a 41/2015 (VII.15.) BM rendelet határozza meg. A szervezet elvárt biztonsági szintjének meghatározását követően a fenti rendeletben foglalt követelmények figyelembe vételével fel kell mérni a szervezet jelenlegi biztonsági szintjét. Jellemzően ez utóbbi nem éri el az elvárt szintet, ezért annak eléréséhez intézkedési tervet kell készíteni.~~

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.2 Az adatok osztályba sorolása, kapcsolódó tevékenységek és szabályok

A 66. oldal táblázata az alábbiak szerint kerül módosításra:

~~Biztonsági osztály~~	~~Osztályba sorolás követelményei~~
~~*1. osztály*~~	~~Ha a szervezet nem üzemeltet és nem fejleszt elektronikus információs rendszert, és saját hatáskörben erre más szervezetet vagy szolgáltatót sem vesz igénybe.~~
~~*2. osztály*~~	~~Ha a szervezet az első szinthez rendelt jellemzőkön túl olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.~~
~~*3. osztály*~~	~~Ha a szervezet második szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe.~~
~~*4. osztály*~~	~~Ha a szervezet a harmadik szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt.~~
~~*5. osztály*~~	~~Ha a szervezet a negyedik szinthez rendelt jellemzőkön túl európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szerveze~~

Biztonsági osztály	*Osztályba sorolás követelményei*
Alap	Ha működése a szervezet szempontjából nem kritikus sem a benne tárolt adatok, sem pedig a funkcionalitás szempontjából. Az alap biztonsági osztályba sorolt rendszer működésének kimaradása nem okozhat egyéb informatikai rendszerek működésében anomáliát.
Jelentős	Ha működése a szervezet üzletmenet szempontjából alapvető mind a benne tárolt adatok, mind pedig a funkcionalitás szempontjából. A jelentős biztonsági osztályba sorolt rendszer működésének kimaradása egyéb informatikai rendszerek működésében csekély zavart vagy üzemkimaradást okozhat.
Magas	Ha működése létfontosságú a szervezet üzletmenet szempontjából a benne tárolt adatok, vagy a funkcionalitás szempontjából. A magas biztonsági osztályba sorolt rendszer működésének kimaradása az egész Társaság működésében jelentős zavart, esetenként leállást okozhat.

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.2.Az adatok osztályba sorolása, kapcsolódó tevékenységek és szabályok

A 67. oldal táblázata az alábbiak szerint kerül módosításra:

	~~1. biztonsági osztály~~	~~2. biztonsági osztály~~	~~3. biztonsági osztály~~	~~4. biztonsági osztály~~	~~5. biztonsági osztály~~
~~adatvesztés~~	~~nem kezel jogszabályok által védett adatot~~	~~személyes adat sérülhet~~	~~különleges személyes adat, vagy nagy mennyiségű személyes adat sérülhet~~	~~különleges személyes adat nagy mennyiségben~~	~~sérülhet különleges személyes adat kiemelkedően nagy mennyiségben sérülhet~~
~~személyi biztonság~~	~~–~~	~~–~~	~~–~~	~~személyi sérülések esélye megnőhet~~	~~emberi élet kerülhet közvetlen veszélybe, nagyszámú sérült várható~~
~~anyagi kár~~	~~az anyagi kár a szervezet költségvetéséhez képest elhanyagolható~~	~~az anyagi kár eléri a szervezet költségvetésének 1 %-át~~	~~az anyagi kár eléri a szervezet költségvetésének 5 %-át~~	~~az anyagi kár eléri a szervezet költségvetésének 10 %-át~~	~~az anyagi kár eléri a szervezet költségvetésének 15 %-át~~
~~nemzeti adatvagyon~~	~~–~~	~~–~~	~~–~~	~~–~~	~~a nemzeti adatvagyon helyreállíthatatlanul sérülhet~~
~~társadalmi működőképesség~~	~~–~~	~~–~~	~~–~~	~~–~~	~~létfontosságú információs rendszer~~

					rendelkezésre állása nem biztosított
társadalmi hatás	káresemény esetén nincs bizalomvesztés	a szervezeten belül kezelhető	bizalomvesztés állhat elő a szervezeten belül	bizalomvesztés a szervezeten belül, jogszabályok betartása elmaradhat	súlyos bizalomvesztés az érintett szervezettel szemben
ügymenet	–	csekély értékű védett adat, vagy elektronikus információs rendszer sérülhet	érzékeny folyamatokat kezelő rendszer vagy információt képező adat sérülhet	nagy értékű információt képező adat, vagy különösen érzékeny adatokat kezelő IT rendszer jelentősen sérülhet	nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő IT rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet
Káresemény	Jelentéktelen	Csekély	Közepes	Nagy	Kiemelkedően nagy

A szervezetek elektronikus rendszereit, illetve azok biztonsági osztályait az informatikai biztonsági szabályzatban kell rögzíteni.

	Alap	Jelentős	Magas
adatvesztés	jogszabály által nem védett adat vagy kis mennyiségű személyes adat sérülhet	nagy mennyiségű személyes adat vagy különleges személyes adat sérülhet	különleges személyes adat nagy mennyiségben sérülhet
személyi biztonság		a személyi sérülés esélye megnőhet	emberi élet kerül közvetlen veszélybe, sérülések nagy számban következhetnek be
anyagi kár	nem haladja meg az éves költségvetés vagy árbevétel 1%-át	meghaladja az éves költségvetés vagy árbevétel 1%-át, de nem haladja meg a 10%/-át	meghaladja az éves költségvetés vagy árbevétel 10%-át
társadalmi hatás	szervezeten belül kezelhető	bizalomvesztés a szervezettel szemben, jogszabályok betartása elmaradhat	súlyos bizalomvesztés a szervezettel szemben, alapvető emberi jogok sérülhetnek

nemzeti adatvagyon	-	-	nemzeti adatvagyon helyreállíthatatlanul megsérülhet
társadalmi működőképesség			kritikus infrastruktúra rendelkezésre állása nem biztosított.
ügymenet	csekély értékű adat vagy rendszer sérülhet	érzékeny folyamatokat kezelő rendszer vagy jogszabály által védett adat sérülhet	nagy értékű üzleti titkot, különösen érzékeny folyamatot kezelő rendszer jelentősen sérülhet
Káresemény	Csekély	Közepes	Nagy

A biztonsági osztályba sorolás eredményét a azelektronikus információs rendszerek nyilvántartásában vagy egyéb belső szabályzatban kell rögzíteni.

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.3. Felelősök, ~~feladatok~~, felelősségi körök

A 68. oldal szövege az alábbiak szerint kerül módosításra:

A törvény és a kapcsolódó végrehajtási rendeletek alapján a szervezetek esetében ~~két~~ több kiemelt ~~felelősségi és feladatkört~~ szerepkört is megkülönböztetünk ~~meg~~:

- a szervezet vezetője,
- az elektronikus információs rendszer biztonságáért felelős személy

A szervezet vezetője: ~~feladatai a legszerteágazóbbak, összefoglalva a szervezet IT-biztonsági környezetének és informatikai rendszerének fenntartásához szükséges személyi és tárgyi feltételek biztosítása.~~

A szervezet vezetőjének felelőssége az irányítása alatt lévő intézmény tekintetében a jogszabályban előírt feladatok elvégzésének biztosítása. Ennek keretében:

- gondoskodik az adatosztályozás elvégzéséről
- gondoskodik a biztonsági osztályba sorolás elvégzéséről
- megbízza az elektronikus információs rendszer biztonságáért felelős személy kijelöléséről.

A jogszabályban előírt feladatok elvégzését az elektronikus információs rendszer biztonságáért felelős személy bevonásával végzi el a szervezet.

Az elektronikus információs rendszer biztonságáért felelős személy: szervezet vezetője az elektronikus információs rendszer védelméhez kapcsolódó feladatok ellátása, a kockázatmenedzsment keretrendszer működtetése, a kiberbiztonsági incidensek bejelentése és a kiberbiztonsági incidenskezelőközponttal való kapcsolattartás érdekében jelöli ki.

Főbb feladatai:

- gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
- gondoskodik a kockázatkezelési keretrendszer szerinti tevékenységek tervezéséről, szervezéséről, koordinálásáról, elvégzéséről és ellenőrzéséről,
- előkészíti és a szervezet vezetőjének jóváhagyását követően megküldi a nemzeti kiberbiztonsági hatóság részére a szervezetinformációbiztonsági szabályzatát,
- előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását,

- előkészíti és a szervezet vezetőjének egyetértésével kezdeményezi a nemzeti kiberbiztonsági hatóságnál a szervezetelektronikus információs rendszereivel kapcsolatos engedélyezési eljárásokat,
- megtartja vagy megszervezi a továbbképzésre kötelezett személyek részére jogszabályban előírt továbbképzéseket,
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet elektronikusinformációbiztonságot érintő szabályzatait és szerződéseit,
- folyamatos és tervezett ellenőrzéseket végez annak vizsgálatára, hogy a szervezet elektronikus információbiztonságra vonatkozó belső normáiban lévő előírások hogyan valósulnak meg, ennek megállapításait írásban rögzíti a szervezet vezetője számára,
- felülvizsgálja, hogy a szervezet elektronikus információbiztonságot érintő belső szabályzatai összhangban vannak-e a hatályosjogszabályokkal és a szervezet belső szabályozóival,
- az ellenőrzések és az esetleges incidensek tapasztalatai felhasználásával – a fejlesztendő területekre vonatkozó javaslatokat tartalmazó – biztonsági helyzetértékelést készít a szervezet vezetője számára,
- legalább évente megvizsgálja a kiberbiztonsági audit során feltárt hiányosságok kapcsán készült intézkedési tervet és beszámolót készít a szervezet vezetője számára az előrehaladásról, amiben kiemeli az esetleges lemaradásokat és a rövid távon szükséges intézkedéseket,
- kapcsolatot tart a nemzeti kiberbiztonsági hatósággal és a kiberbiztonsági incidenskezelő központtal,
- a szervezet bármely elektronikus információs rendszerét érintő incidensről tájékoztatja e rendeletben meghatározott szervet,
- együttműködik az ellenálló képességéért felelős vezetővel.

~~Legfontosabb feladatai:~~
~~• biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését;~~
~~• biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését;~~
~~• elektronikus információs rendszer biztonságáért felelős személyt nevez ki, vagy bíz meg;~~
~~• kiadja az informatikai biztonsági szabályzatot, és kijelöli az ehhez kapcsolódó felelősöket;~~
~~• gondoskodik a rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról;~~
~~• gondoskodik a rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatásáról;~~
~~• gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről;~~
~~• biztonsági esemény bekövetkezésekor gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, a biztonsági események kezeléséről;~~
~~• ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy a törvényben foglaltak szerződéses kötelemként teljesüljenek;~~
~~• ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy a törvényben foglaltak szerződéses kötelemként teljesüljenek;~~
~~• felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért;~~
~~• megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.~~
~~Az elektronikus információs rendszer biztonságáért felelős személy: a szervezet keretein belül tevékenykedik. Feladatvégzése során közvetlenül tájékoztathatja a szervezet vezetőjét.~~

~~Legfontosabb feladatai:~~
~~• gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról;~~
~~• elvégzi vagy irányítja az előző pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését;~~
~~• előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot;~~
~~• előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását~~

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.3. Felelősök, ~~feladatok~~, felelősségi körök

A 69. oldal szövege az alábbiak szerint kerül módosításra:

~~• véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit;~~
~~• kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.~~

Kiberbiztonsági audit
A jogszabály hatálya alá tartozó szervezetek rendszeres időközönkét kötelesek elektronikus információs rendszereik kiberbiztonsági megfelelőségét vizsgáltatni. Ez a vizsgálat a kiberbiztonsági audit. Ennek során a vizsgálatot végző szervezet a vizsgálat tárgyát képező elektronikus információs rendszer szabályozási környezetének dokumentációjának, felépítésének, konfigurációs beállításainak és sérülékenységének vizsgálatával ellenőrzi a rendszer megfelelőségét.

~~Az elektronikus információs rendszer biztonságának felügyelete~~
~~Az elektronikus információs rendszerek biztonsági felügyeletét a Kormány által kijelölt hatóság látja el.~~
~~A hatóság legfontosabb feladatai:~~
~~• az osztályba sorolás és a biztonsági szint megállapításának ellenőrzése és az ellenőrzés eredménye alapján döntés meghozatala,~~
~~• az elektronikus információs rendszerek osztályba sorolására és a szervezetek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzése,~~
~~• az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése, és eredményességének ellenőrzése,~~
~~• a rendelkezésre álló információk alapján kockázatelemzés elvégzése,~~
~~• a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálása hatósági eljárás keretében,~~
~~• javaslattétel a létfontosságú rendszerek és létesítmények ágazati kijelölő hatósága részére a nemzeti létfontosságú rendszerelem kijelölésére,~~
~~• együttműködés az elektronikus ügyintézési felügyelettel a szabályozott elektronikus ügyintézési szolgáltatás szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében,~~
~~• kapcsolattartás az elektronikus információbiztonság területén a nemzetbiztonsági szolgálatokkal,~~
~~• kapcsolattartás az eseménykezelő központokkal.~~

Információbiztonsági felügyelő
Az információbiztonsági felügyelőt a- nemzeti kiberbiztonsági hatóság ~~hatóság javaslatára az e-közigazgatásért felelős miniszter~~ jelöli ki abban az esetben, ha egy szervnél a biztonsági követelményeket, illetve az ahhoz szükséges szabályokat nem tartják be. Az információbiztonsági felügyelő feladata az érintett szervezet bevonásával a nemzeti

kiberbiztonsági hatóság által meghatározott határidőn belül intézkedési tervet készíteni a nemzeti kiberbiztonsági hatóság általmegjelölt hiányosságok felszámolása érdekében. ~~Az információbiztonsági felügyelő a hatóság által jóváhagyott intézkedési tervalapján jár el.a szervezet elektronikus információs rendszereinek védelmét biztosítani az esetleges biztonsági fenyegetésekkel szemben, valamint helyreállítani az adott kormányzati szerv elektronikus információs rendszerének előírt biztonsági szintjéhez szükséges informatikai környezetet~~.

~~Kormányzati eseménykezelő központ~~

~~Az a szervezet, amely nyilvántartja az érintett szerveknél bekövetkező biztonsági eseményeket, és szükség esetén támogatást nyújt a kárfelmérésben és a következmények kezelésében. Emellett folyamatos hálózatbiztonsági elemzéseket végez, azonnali értesítést ad a kritikus hálózatbiztonsági eseményekről. A nemzetközileg publikált sérülékenységeket közzéteszi a honlapján. Rendszeres időközönként információbiztonsági és katasztrófa elhárítási gyakorlatokat szervez.~~

Kiberbiztonsági incidenskezelő központok
Alapvetően ágazati, honvédelmi és nemzeti kiberbiztonsági incidenskezelő központokat különböztetünk meg. Főbb feladataik:

- kiberteret érintő fenyegetésekkel és a kiberbiztonsági incidensek megelőzésével kapcsolatos feladatok ellátása
- kiberbiztonsági incidenskezeléshez kapcsolódó feladatok ellátása
- kiberbiztonsági válsághelyzetek kezelése
- sérülékenységeket, sebezhetőségeket érintő feladatok ellátása
- tájékoztatási, tudatosító tevékenységek végrehajtása
- az európai uniós és nemzetközi együttműködés

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.3. Felelősök, ~~feladatok~~, felelősségi körök

A 70. oldal szövege az alábbiak szerint kerül módosításra:

Figyelembe véve, hogy a jogszabály hatálya igen sok különböző ágazathoz kapcsolódó szervezetre terjed ki, ezért az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságokat a jogszabály az alábbiak szerint jelölte ki:

- A közigazgatási ágazatokhoz tartozó szervezetek, illetve a többségi állami tulajdonú szervezetek esetében a Nemzeti kiberbiztonsági hatóság
- A kiemelten kockázatos és kockázatos ágazatokban működő szervezetek esetében az Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH)
- A honvédelmi célú elektronikus információs rendszerek esetében a honvédelmi kiberbiztonsági hatóság

Nemzeti kiberbiztonsági hatóságként a Kormány a Nemzetbiztonsági szolgálatot jelölte ki.

~~Az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóságként a Kormány a Nemzetbiztonsági Szakszolgálatot jelöli ki.~~

A Nemzeti Kiberbiztonsági Hatóság jogosult

- a biztonsági osztályba sorolást, a védelmi intézkedéseket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,
- a minimálisan elvárt védelmi intézkedéseket meghatározni,
- a szervezet által meghatározott biztonsági osztályhoz tartozó védelmi intézkedéseken túl további biztonsági követelményeket meghatározni,
- a szervezet által elfogadott kiberbiztonsági kockázatkezelési intézkedések értékeléséhez, valamint az információk bejelentésére vonatkozó kötelezettség betartásának értékeléséhez szükséges tájékoztatást kérni,

- a védelmi intézkedések és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,
- rendszeres, eseti és célzott biztonsági ellenőrzéseket végezni, ideértve a helyszíni ellenőrzéseket, a távoli felügyeleti intézkedéseket és a véletlenszerű ellenőrzéseket is,
- a felügyeleti feladatai ellátásához szükséges adatokhoz, dokumentumokhoz és információkhoz hozzáférni és ezeket bekérni, illetve a megküldött dokumentumok felülvizsgálatát elrendelni,
- eljárása során független értékelőt igénybe venni, és az általa végzett ellenőrzés eredményét, továbbá a szervezet által megbízott független értékelő jelentésében vagy a kiberbiztonsági auditjelentésben foglaltakat figyelembe venni,
- az elektronikus információs rendszerekre és eszközökre, a szervezetekre nemzetközi egyezmények vagy nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján kiadott biztonsági tanúsítványokat figyelembe venni,
- európai uniós szerződése, rendeletek, irányelvek, határozatok, ajánlások által meghatározott kiberbiztonsági követelményeknek való megfelelést részben vagy egészben az informatikáért felelős miniszter rendeletében meghatározott védelmi követelményeknek való megfelelésnek tekinteni,
- az ellenőrzés során feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni,
- a felügyeleti jogkörébe tartozó szervezetek vonatkozásában szabvány alkalmazására, európai vagy hazai kiberbiztonsági tanúsítási rendszerek által tanúsított információs és kommunikációs technológiai termék használatára, illetve minősített bizalmi szolgáltatás igénybevételére iránymutatásokat kiadni,
- az elektronikus információs rendszerek használatba vételének, meglévő elektronikus információs rendszer továbbhasználatának jóváhagyása során helyszíni ellenőrzést tartani és sérülékenységvizsgálatot elrendelni,
- a Központ megkeresése alapján a szervezet elektronikus információs rendszere kapcsán bejelentett sérülékenységfelszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni, illetve egyedi mérlegelés alapján sérülékenységvizsgálatot elrendelni.

A nemzeti kiberbiztonsági hatóság feladatai ellátása során együttműködik az elektronikus információbiztonság területén

- a kiberbiztonsági incidenskezelő központokkal,
- a kiberbiztonsági tanúsító hatósággal,
- a kapcsolódó jogszabályok szerinti kijelölő hatóságokkal és szakhatóságokkal,
- a rendvédelmi szervekkel,
- a nemzetbiztonsági szolgálatokkal,
- a katonai kibertér műveleti erőkkel,
- a Nemzeti Média- és Hírközlési Hatósággal,
- a Nemzeti Adatvédelmi és Információszabadság Hatósággal,
- az Európai Unió tagállamainak vagy harmadik országok kiberbiztonsági felügyeleti hatóságaival, valamint
- más tagállamok illetékes hatóságaival.

~~Fontosabb feladatai:~~

~~• az európai államok területén az elektronikus információs rendszer üzemeltetését engedélyezi, az üzemeltetést ellenőrzi;~~

~~• az IT-fejlesztési projekttervekben ellenőrzi az információbiztonsági követelmények teljesülését;~~

~~• nyilvántartja a szervek elektronikus információs rendszereinek adatait;~~

~~• nyilvántartja és közzéteszi a biztonsági eseményekkel kapcsolatos értesítéseket;~~

~~• hatósági eljárás keretében fizikai, logikai és adminisztratív védelmi ellenőrzéseket végez;~~

~~• szükség szerint konzultációt folytat és együttműködik a rendvédelmi szervekkel, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósággal;~~

~~• az elektronikus információs rendszerek biztonságáért felelős nemzetközi szervezetekben képviseli Magyarországot.~~

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény és a 418/2024 (XII.23) Kormányrendelet hatályba lépése

2.5.4. Biztonsági esemény és kezelése

A 70. oldal szövege az alábbiak szerint kerül módosításra:

2.5.4. ~~Biztonsági esemény~~ Kiberbiztonsági incidens és kezelése

~~Biztonsági esemény~~ Kiberbiztonsági incidens: olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát

~~olyan nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.~~

Kiberbiztonsági incidenskezelés: minden olyan tevékenység és eljárás, amelynek célja a kiberbiztonsági incidens megelőzése, észlelése, elemzése és elszigetelése vagy a kiberbiztonsági incidensre való reagálás és a kiberbiztonsági incidenst követően a működés helyreállítása. ~~Biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység~~. Minden, a törvény hatálya alá tartozó szervezet az elektronikus információs rendszerében bekövetkezett kiberbiztonsági incidensről ~~biztonsági eseményről~~ köteles az ágazati eseménykezelő központot értesíteni. Amennyiben nincs ágazati eseménykezelő központ, úgy a jelentési kötelezettség a kormányzati eseménykezelő központ felé él. A mindennapokban a kiberbiztonsági incidens ~~biztonsági esemény~~ többnyire a munkaállomások vírusfertőzése, adathalászlevelek rendszerbe érkezése vagy valamilyen természeti katasztrófa okozta szolgáltatáskiesés lehet. Minden ilyen eset bekövetkezését követően egy jól meghatározott folyamat indul el az intézményeknél, mely amellett, hogy a rendszer működőképességének mielőbbi helyreállításáról intézkedik, az incidens ~~esemény~~ pontos dokumentálására is figyelmet fordít. Ez azért fontos, hogy a későbbiekben az incidens ~~esemény~~ okait ki lehessen vizsgálni.

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.5. Kiberbiztonsági tanúsítás

A 70. oldal szövege az alábbiak szerint kerül módosításra

2.5.5. Kiberbiztonsági tanúsítás

~~A tanúsítási tevékenység célja, hogy az Európai Uniós elvárásoknak megfelelően a digitális eszközök és szolgáltatások esetében garantálni lehessen a kiberbiztonsági védelmet~~. ~~Az eszközökön elhelyezett tanúsítvány azt a célt szolgálja, hogy egyértelműen felismerhetővé tegye a biztonság szintjét a felhasználók számára, továbbá garantálja azt, hogy a termék megfelel az Európai Unió által meghatározott követelményeknek~~.

A tanúsítási tevékenység célja az, hogy az állampolgárok és a vállalkozások által megvásárolható, igénybe vehető infokommunikációs eszközök és szolgáltatások esetében garantálni lehessen a kiberbiztonság folyamatosan fejlődő követelményeinek való megfelelést. A tanúsítványban foglalt információk birtokában a fogyasztó szabadon

eldöntheti, hogy milyen erős kiberbiztonsági képességgel bíró terméket kíván megvásárolni és használni a jövőben.

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.5. Kiberbiztonsági tanúsítás

A 71. oldal szövege az alábbiak szerint kerül módosításra

~~A kiberbiztonsági tanúsítás önkéntes, kivéve, ha erről hazai vagy uniós jogszabály eltérően rendelkezik. Tanúsításra megfelelőségértékelési szervezet vagy tanúsító hatóság jogosult. Alap megbízhatósági szintű IKT termékek, szolgáltatások vagy folyamatok esetében a jogszabály lehetővé teszi a gyártók számára a megfelelőségi önértékelést, mely alapján a gyártó uniós megfelelőségi nyilatkozatot adhat ki.~~ ~~A tanúsító hatóság nyilvántartást vezet:~~
~~– a megfelelőségértékelési szervezetekről,~~
~~– a megfelelőség önértékelést végző szervezetekről.~~
~~Ezen felül a tanúsító hatóság ellenőrzési jogkörrel is rendelkezik, melynek keretében vizsgálhatja, hogy:~~
~~– a megfelelőségi tanúsítvánnyal ellátott termékek valóban megfelelnek-e a vonatkozó előírásoknak,~~
~~– illetve piacfelügyeleti ellenőrzéseket is végez.~~

Nemzeti kiberbiztonsági tanúsítási rendszert kell létre hozni, mely a jogszabályban definiált biztonsági célokat kell teljesítenie.
A nemzeti kiberbiztonsági tanúsítási rendszer tanúsítási rendszer az infokommunikációs eszközök és szolgáltatások tekintetében alábbi megbízhatósági szintek közül határoz meg egy vagy több szintet:

- alap: alap megbízhatósági szinten a rendszer teljesíti azokat a biztonsági követelményeket, melyek alkalmasak a biztonsági eseményekkel és támadásokkal kapcsolatos alapvető, ismert kockázatok minimalizálására
- jelentős: jelentős megbízhatósági szinten a rendszer teljesíti azokat a biztonsági követelményeket, melyek alkalmasak az ismert kiberbiztonsági kockázatok, valamint a korlátozott szakértelemmel és erőforrásokkal rendelkező elkövetők által végrehajtott biztonsági események és kiberbiztonsági támadások kockázatának minimalizálására
- magas: magas megbízhatósági szinten a rendszer teljesíti azokat a biztonsági követelményeket, melyek alkalmasak jelentős szakértelemmel és erőforrásokkal rendelkező elkövetők által, a tudomány legutolsó állása szerinti technológiával végrehajtott kibertámadások kockázatának minimalizálására.

A kiberbiztonsági tanúsítás hatósági feladatait – a hadiipari termékek kivételével – a Szabályozott Tevékenységek Felügyeleti Hatósága látja el.

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

2.5.6. Poszt-kvantumtitkosítás

A 71. oldal szövege az alábbiak szerint kerül módosításra

2.5.6. Poszt-kvantumtitkosítás

A poszt-kvantumtitkosítás olyan titkosítási eljárás, mely biztosítja hogy az elektronikus adatok és kommunikációs csatornák kvantumszámítógép okozta kibertámadás ellen is védettek legyenek. Ezt a védelmi szintet a hagyományos titkosítási eljárások nem tudják biztosítani, mert a kvantumszámítógép képes lehet olyan számítások hatékony végzésére, amik a hagyományos, digitális számítógépekkel gyakorlatilag megoldhatatlanok. Ezért szükséges olyan új eljárások kidolgozása és bevezetése az elektronikus adattárolás és kommunikáció során, mely megfelelő szintű védelmet biztosít ezen eszközök esetében is.

Azon szervezeteket, melyek részére jogszabály kötelezően előírja a post-kvantumtitkosítás alkalmazását poszt-kvatnumtitkosítás alkalmazására kötelezett szervezeteknek hívjuk.
A poszt-kvantumtitkosítás alkalmazására kötelezett szervezet elektronikus információs rendszere teljes életciklusában biztosítani kell :

- a rendszerben kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását,
- a rendszer hagyományos kriptográfiai alkalmazáson felüli biztonságot nyújtó poszt-kvantumtitkosítási alkalmazással történő zárt, teljes körű, folytonos és a kockázatokkal arányos védelmét.

A szolgáltatást ezek a szervezetek poszt-kvantumtitkosítást nyújtó szolgáltatótól is igénybe vehetik. Szolgáltató csak olyan szervezet lehet, amely:
– nemzetbiztonsági kockázatot nem jelent;
– telephely biztonsági tanúsítvánnyal rendelkezik;
– munkavállalói személyi biztonsági tanúsítvánnyal rendelkeznek;
– által használt informatikai rendszer biztosítja a rendszerelemek zártságát, és megakadályozza az informatikai rendszerhez történő jogosulatlan hozzáférést, valamint észrevétlen módosítását. A poszt-kvantumtitkosítás alkalmazást nyújtó szervezet informatikai rendszerének a magas információbiztonsági követelményein túl meg kell felelnie az általános információbiztonsági zártsági követelményeknek is.
– szerepel a tanúsító szervezet nyilvántartásában;
– az általa nyújtott alkalmazás rendelkezik a tanúsító szervezet megfelelőséget igazoló szakvéleményével.

Indokolás: jogszabályváltozás, a 2024. évi LXIX. törvény hatályba lépése.

3.1. ELEKTRONIKUS ÜGYINTÉZÉS

A 73. oldal szövege az alábbiak szerint kerül módosításra:

3.1. ELEKTRONIKUS ÜGYINTÉZÉS – Digitális állampolgárság
Az elektronikus ügyintézés során a felhasználó a digitális szolgáltatást nyújtó szervezet előtt az ügyei digitális térben történő intézése során ügyintézési cselekményeit a jogszabály szerint, elektronikusan végzi, nyilatkozatait elektronikus úton teszi meg. ~~az ügyfél bármely hatóság vagy gazdálkodási szerv felé irányuló ügyintézési tevékenysége, melyet elektronikus eszköz segítségével végez. Az elektronikus ügyintézés technikájának és folyamatainak szabályozására 2015. december 15-én elfogadásra került az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény.~~ A hatósági ügyek elektronikus ügyintézését a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény, illetve a kapcsolódó 321/2024. (XI. 6.) Korm. rendelet szabályozza.
Az elektronikus ügyintézés használatát a jogszabály esetenként korlátozza.
Nem alkalmazható elektronikus ügyintézés

- ha jogszabály kifejezetten a felhasználó személyes megjelenését írja elő,
- amennyiben ez nem értelmezhető az eljárásban
- amennyiben nemzetközi szerződés, vagy az EU általános hatályú, közvetlenül alkalmazandó kötelező jogi aktusa kizárja
- olyan irat, okirat vagy más beadvány esetében, mely minősített adatot tartalmaz.

~~• ha az ügyfél személyes jelenléte vagy az okiratok személyes benyújtása elengedhetetlen;~~
~~• azon esetekben, ahol az elektronikus ügyintézés az eljárás során nem értelmezhető,~~
~~• abban az esetben, ha ezt nemzetközi szerződés vagy az Európai Unió általános hatályú jogi aktusa kizárja;~~
~~• ha az ügyintézés során bármely okirat minősített adatot tartalmaz;~~
~~• diplomáciai és sportdiplomáciai ügyekben.~~

A jogszabály alapján elektronikus ügyintézésre kötelezettek az alábbiak:

- a felhasználóként eljáró
- gazdálkodó szervezet,
- az államháztartásról központi és önkormányzati szervezetei,
- ügyész,

- jegyző,
- egyéb közigazgatási hatóság, valamint
- a felhasználó jogi képviselője.

~~A törvény alapján az elektronikus ügyintézés alapelvei:~~
~~• az ügyfelet megilleti a jog, hogy ügyeit elektronikusan intézze;~~
~~• az elektronikus ügyintézésre az ügyintéző szerv az általánosnál rövidebb ügyintézési időt is vállalhat, amennyiben az nem befolyásolja negatívan a többi ügy ügyintézési határidejét;~~
~~• elektronikus ügyintézés esetén az ügyfél részére nem határozható meg kötelezően használandó technikai megoldás;~~
~~• elektronikus ügyintézésben mindkét fél köteles a jóhiszeműség, tisztesség és kölcsönös együttműködés követelményeinek megfelelően eljárni;~~
~~• az elektronikus ügyintézési rendszerek folyamatait az ügyfél érdekeinek figyelembe vételével kell kialakítani;~~
~~• az ügyintézési folyamat során biztosítani kell a közérdekű, illetve közérdekből nyilvános adatok megismerhetőségét, valamint a személyes, minősített és nem nyilvános adatok védelmét;~~
~~• nem alkalmazható elektronikus ügyintézés olyan eljárások esetében, ahol a jogszabály személyes megjelenést vagy okiratok személyes benyújtását írja elő.~~

A digitális állampolgárság program lényege, hogy minden a személyi adat nyilvántartásban szereplő állampolgár független digitális térben alkalmazható azonosítót kap, melynek segítségével igénybe tudja
venni a számára nyújtott digitális szolgáltatásokat.
Emellett létre hozásra került a digitális állampolgárság nyilvántartás – amely egy ügyfél regisztrációs nyilvántartásnak menősül –, mely az alábbi célokat szolgálja:
– a felhasználó felhasználói profilja aktív vagy inaktív státuszával, a digitális állampolgár azonosítóval, valamint a nyilvántartásban tárolt egyéb adatokkal kapcsolatos adatszolgáltatások teljesítése,
– a Kormány által kötelezően biztosított elektronikus azonosítási szolgáltatás kapcsán annak hiteles biztosításához és mások jogának vagy jogos érdekének védelme érdekében az érintett személy azonosításához szükséges adatok és technikai azonosítók közhiteles kezelése.
A digitális állampolgárság keretében az alábbi szolgáltatások igénybe vétele lehetséges:

- digitális keretszolgáltatások: A digitális állampolgárság program igénybe vételéhez szükséges alapvető szolgáltatások összessége. Részei:
  - eAzonosítás
  - eAláírás
  - ePosta
  - eDokumentumkezelés
  - eFizetés
- élet-esemény alapú szolgáltatások: ezen szolgáltatások az ember élete során előforduló fontosabb történésekhez, változásokhoz kapcsolódó hatósági ügyek kezelését teszik lehetővé.

Indokolás: jogszabályváltozás, a 2023. évi CIII. törvény módosítása.

3.1.3 SZEÜSZ

A 76. oldal szövege az alábbiak szerint kerül módosításra:

3.1.3. SZEÜSZ
A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) 2011. évi módosítása vezette be a SZEÜSZ fogalmát, melyet a 2013. január 1-jével hatályba lépett módosítás újabb szolgáltatásokkal egészített ki. A SZEÜSZ ~~szabályait az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 2017. január 1-jével hatályba lépő rendelkezései módosítják.~~ szabályait a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény rendelkezései határozzák meg.

A SZEÜSZ olyan elektronikus ügyintézést megkönnyítő szolgáltatás, amely az ügyfélközpontú ügyintézési megközelítésnek rendeli alá a szolgáltatók informatikai infrastruktúráját, meghatározva ezzel annak fejlesztési irányait és biztonsági követelményeit.

A jogszabály alapján az alábbi kötelezően biztosított SZEÜSZ-ök léteznek:

- ~~**Elektronikus azonosítási szolgáltatás:** *a természetes vagy jogi személyt, illetve jogi személyt képviselő természetes személyt egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata.*~~
- ~~**Biztonságos kézbesítési szolgáltatás:** *olyan kézbesítési szolgáltatás, amely az elektronikus küldemény kézbesítésével kapcsolatosan megfelel az alábbi feltételeknek:*~~
  - ~~*a) ha a küldőtől átvett üzenetet változatlan formában a címzett rendelkezésére bocsátották, akkor erről a küldő számára legalább fokozott biztonságú elektronikus aláírással ellátott elektronikus dokumentumba foglalt igazolás álljon rendelkezésre;*~~
  - ~~*b) az üzenet és a kézbesítést igazoló okirat észrevétlenül nem megváltoztatható sem a kézbesítés során, sem a kézbesítést követően,*~~
  - ~~*c) az üzenet átvevője csak a címzett vagy a feljogosított helyettes átvevő lehet, és a tényleges átvevő személyét az átvétellel kapcsolatos okirat igazolja,*~~
  - ~~*d) a feladónak okirati bizonyíték áll rendelkezésére (tértivevény) arról az esetről is, ha a kézbesítés a megadott időn belül sikertelen; az igazolás a meghiúsulás időpontját és – ha azonosítható – okát tartalmazza.*~~
- ~~**Kormányzati hitelesítés szolgáltatás:** *Az elektronikus ügyintézési törvény által szabályozott elektronikus aláírással kapcsolatos szolgáltatásokat a kormányzati hitelesítés szolgáltató nyújtja.*~~
- ~~**Kormányzati elektronikus aláírás és aláírás-ellenőrzési szolgáltatás:** *a szolgáltatás keretében a szolgáltató biztosítja az elektronikus dokumentumon elhelyezett elektronikus aláírás, elektronikus bélyegző érvényességének ellenőrzését, valamint az elektronikus ügyintézést biztosító szerv számára elérhetővé teszi a dokumentum elektronikus aláírással vagy elektronikus bélyegzővel, valamint időbélyegzővel történő hitelesítését.*~~
- az elektronikus azonosítási szolgáltatás: *eAzonosítás, illetve az emelt szintű kétfaktoros azonosítást biztosító ügyfélkapu.*
- az ajánlott elektronikus kézbesítési szolgáltatás,
- Kormányzati hitelesítés szolgáltatás:
  - elektronikus aláírás és elektronikus bélyegző szolgáltatások
  - elektronikus időbélyegző szolgáltatás
  - titkosítási célú tanúsítványok kibocsátása
  - tanúsítványok érvényességének igazollása.
- az e törvény felhatalmazása alapján kiadott kormányrendeletben szabályozott elektronikus ügyintézési szolgáltatásként nevesített szolgáltatás.

Indokolás: jogszabályváltozás, a 2023. évi CIII. törvény módosítása.

3.1.3 SZEÜSZ

A 77. oldal szövege az alábbiak szerint kerül módosításra:

- ~~Kézbesítési szolgáltatás: a szolgáltató az elektronikus nyilatkozatok kézbesítésének folyamatában részt vesz, átveszi, továbbítja vagy tárolja az üzeneteket.~~
- ~~Hivatali tárhely: a kézbesítési szolgáltatáshoz kapcsolódó hivatali tárhely a kijelölt szolgáltató által az elektronikus ügyintézést biztosító szervek számára nyújtott hivatalos elektronikus kapcsolattartásra szolgáló tárhely, biztonságos kézbesítési szolgáltatási cím.~~
- ~~KÜNY regisztrációhoz kapcsolódó tárhely: biztonságos kézbesítési szolgáltatási címnek minősülő, a KÜNY regisztrációhoz kapcsolódó tárhely szolgáltatás kijelölt~~

~~szolgáltatója az ügyfél részére a biztonságos kézbesítési szolgáltatáshoz kötődő tárhelyet biztosít.~~

- ~~Gazdálkodó szervezetek számára biztosított tárhely: a kézbesítési szolgáltatáshoz kötődő, biztonságos kézbesítési szolgáltatási címnek minősülő tárhely, cégkapu.~~

Elektronikus azonosítási szolgáltatás
Az elektronikus azonosítási szolgáltatást az veheti igénybe, aki regisztrál a szolgáltatás igénybevételére és szerepel az elektronikus azonosítási szolgáltató ügyfél-regisztrációs nyilvántartásában ~~adatbázisában~~.
Az ügyfél regisztrálhat:
• elektronikusan, elektronikus azonosító eszköz segítségével,
• személyes megjelenéssel a regisztrációs szerv előtt.
Az elektronikus azonosítási szolgáltató az igénylőkről nyilvántartást, ügyfél-regisztrációs nyilvántartást vezet. A nyilvántartás az alábbi adatokat tartalmazza:
• az igénylő természetes személy azonosító adatait,
• állampolgárságát,
• egyedi azonosító számát,
• külföldi személy esetén a regisztrációhoz használt okmány számát, típusát és érvényességi idejét.

A regisztráció megszűnik:
- a felhasználó kérelmére,
- a felhasználó halála esetén,
- külföldi személyek esetén a regisztrációhoz használt okmány érvényességének lejártával,
- illetve abban az esetben is, ha a regisztrációs szerv arról értesül, hogy az ügyfél nem szerepel az alábbi nyilvántartások egyikében sem:
  - személyiadat- és lakcímnyilvántartás
  - központi idegenrendészeti nyilvántartás
  - elektronikus ügyintézést igénybe vevő külföldi személyek nyilvántartása.

Az ügyfelek az elektronikus ügyintézés keretében központi elektronikus ügyintézési szolgáltatásokat (KEÜSZ) vehetnek igénybe. A Kormány által jogszabályban kijelölt szolgáltató útján biztosított központi elektronikus ügyintézési szolgáltatások az alábbiak:

- **Az ügyfél ügyintézési rendelkezésének nyilvántartása**: *tartalmazza az ügyfél jognyilatkozatait az elektronikus kapcsolattartás módjával, lehetőségeivel, illetve az elektronikus kapcsolattartás ügyfelet érintő naplózásával és értesítéseivel kapcsolatosan.*
- **Iratérvényességi nyilvántartás***: a nyilvántartás a hatóság által kiadmányozott elektronikus dokumentumok, illetve ezekről az elektronikus dokumentumokról készített papíralapú hiteles másolatok tartalmának és hitelességének ellenőrzését biztosító ny*ilvántartás.
- ~~**Elektronikus fizetési és elszámolási rendszer**: *az EFER működtetője az EFER igénybevételével történő fizetés érdekében megállapodást köt azon banki szolgáltatóval, amely a megállapodásban vállalja, hogy a szervezetekkel való kapcsolattartásra az erre a célra biztosított csatlakozófelületet használja, és megfelel a kormányzati portálon közzétett technikai feltételrendszernek.*~~
- ***eFizetés****: digitális keretszolgáltatásként elérhető fizetési szolgáltatás.*

Indokolás: jogszabályváltozás, a 2023. évi CIII. törvény módosítása.

3.1.3 SZEÜSZ

A 78. oldal szövege az alábbiak szerint kerül módosításra:

- **Papíralapú irat átalakítása hiteles elektronikus irattá:** *a szolgáltató az ügyfél által benyújtott papíralapú iratokról hiteles elektronikus másolatot készít.*
- **Elektronikus irat hiteles papíralapú irattá alakítása:** *az elektronikus ügyintézést biztosító szerv olyan papír alapú kivonatot/másolatot készít az elektronikus dokumentumról, amely hivatalos felhasználásra alkalmas.*
- **Központi azonosítási ügynök:** *a jogszabályban kijelölt szervezet a hatóságok részére kötelezően nyújtandó azonosság-ellenőrző ügynöki szolgáltatást nyújt KAÜ szolgáltatásként, mely magában foglalja az ügyfélkapus jelszavas azonosítást, valamint a kormány által kötelezően nyújtott személyazonosításokat.*
- **Személyre szabott ügyintézési felület:** *olyan internetes felület, amely az ügyfél számára személyre szabható módon biztosítja az elektronikus ügyintézéshez szükséges kötelezettségek teljesítését és az elektronikus ügyintézési szolgáltatások igénybevételét.*
- **Űrlapbenyújtási támogatási szolgáltatás***: Az e-Űrlap szolgáltatás biztosítja a jogszabályban meghatározott szerv vagy szolgáltató meghatározott technikai előírásoknak megfelelő elektronikus űrlapok ügyfél általi kitöltését.*
    - *központi azonosítási ügynök szolgáltatáson keresztül érhető el,*
    - *a szolgáltató biztosítja a megfelelő elektronikus űrlapot, illetve hozzá elektronikus dokumentumok csatolhatóságát,*
    - *a szolgáltatás része az űrlap és a csatolt dokumentumok átadása a biztonságos kézbesítési szolgáltatás részére,*
    - *a szolgáltató biztosíthatja az űrlap adatokkal történő kiegészítését az azonosításkorhasznált adatok alapján,*
    - ○ *az űrlap automatikusan kitöltendő részei csak olyan adatokat tartalmaznak, melyre az érintett szervezet adatkezelési jogosultsága fennáll.*
- **ePapír:** *Az e-Papír egy ingyenes, hitelesített üzenetküldő alkalmazás, amely internetkapcsolaton keresztül, elektronikus úton összeköti az Ügyfélkapuval rendelkező ügyfeleket a szolgáltatáshoz csatlakozott intézményekkel*.
- **Összerendelési nyilvántartás***: a szolgáltató összerendelési nyilvántartást vezet valamennyi élő természetes személyre vonatkozóan –beleértve a Magyarországon élő magyar és külföldi, illetve a külföldön élő magyar állampolgárokat – a vonatkozó nyilvántartások alapján. A nyilvántartásból a jogosult szervezeteke számára adatot szolgáltat.*
- **szerepkör-tanúsító platform szolgáltatás***: A szolgáltatás a tanúsítvány alany szerepkörének tanúsításában közreműködő elektronikus ügyintézési szolgáltatás. A számítógéppel értelmezhető elektronikus dokumentumon az alany szerepkörét tanúsító rövid életű tanúsítványt állít ki.*
- ***Szerepkör-tanúsítási szolgáltatás****: a szerepkör tanúsítvány szolgáltató az ügyintézési folyamat során az elektronikus dokumentumokon szabványos, géppel értelmezhető, az érintettnek az eljárásban betöltött szerepkörét tanúsító rövid érvényességű tanúsítványt állít ki.*
- **automatikus közigazgatási döntéshozatali rendszer:** *Azon közigazgatási ügyek tekintetében, ahol ezt jogszabály megengedi és minden szükséges adat rendelkezésre áll, a hatóság emberi beavatkozás nélkül meghozza döntését.*
- **a Kormány által rendeletben megjelölt központi elektronikus ügyintézési szolgáltatás***:*
- ~~**Azonosításra visszavezetett dokumentumhitelesítés***: a szolgáltatás keretében a szolgáltató az ügyfél által rendelkezésre bocsátott nyilatkozatot az általa igazolt személyhez rendeli, majd a személyhez rendelést hitelesen igazolja.*~~
- ~~**Ügyfél időszaki értesítése az elektronikus ügyintézési cselekményekről***: lényege, hogy az ügyfelet a megadott értesítési címen rendszeres időközönként tájékoztatják arról, hogy meghatározott hatóságok az ügyféltől elektronikus vagy papíralapú nyilatkozatot kaptak-e, illetve adtak-e ki. Az értesítés összesített darabszámot tartalmaz.*~~

- ~~**Papíralapú irat átalakítása hiteles elektronikus irattá:** *a szolgáltató az ügyfél által benyújtott papíralapú iratokról hiteles elektronikus másolatot készít.*~~
- ~~**Elektronikus irat hiteles papíralapú irattá alakítása:** *az elektronikus ügyintézést biztosító szerv olyan papír alapú kivonatot/másolatot készít az elektronikus dokumentumról, amely hivatalos felhasználásra alkalmas.*~~
- ~~**Központi azonosítási ügynök:** *a jogszabályban kijelölt szervezet a hatóságok részére kötelezően nyújtandó azonosság-ellenőrző ügynöki szolgáltatást nyújt KAÜ szolgáltatásként, mely magában foglalja az ügyfélkapus jelszavas azonosítást, valamint a kormány által kötelezően nyújtott személyazonosításokat.*~~
- ~~**Személyre szabott ügyintézési felület:** *olyan internetes felület, amely az ügyfél számára személyre szabható módon biztosítja az elektronikus ügyintézéshez szükséges kötelezettségek teljesítését és az elektronikus ügyintézési szolgáltatások igénybevételét.*~~
- ~~**Általános célú elektronikus kéreleműrlap szolgáltatás***: a szolgáltatás lehetővé teszi, hogy ügyfél az elektronikus ügyintézést biztosító szervhez szabad szöveges beadványt terjesszen elő, amennyiben ezt jogszabály engedélyezi és egyéb formai követelményeket nem határoz meg.*~~
- ~~**Összerendelési nyilvántartás***: a szolgáltató összerendelési nyilvántartást vezet valamennyi élő természetes személyre vonatkozóan - beleértve a Magyarországon élő magyar és külföldi, illetve a külföldön élő magyar állampolgárokat – a vonatkozó nyilvántartások alapján. A nyilvántartásból a jogosult szervezeteke számára adatot szolgáltat.*~~
- ~~**Központi kormányzati szolgáltatási busz***: tanúsítvány alapú titkosított adatforgalom segítségével biztosítja az E-ügyintézési törvényben előírt informatikai együttműködés biztonságos feltételeit. Kizárólag adattovábbítást végez, a továbbított üzenet tartalmát nem ismeri.*~~

Indokolás: jogszabályváltozás, a 2023. évi CIII. törvény és a 322/2024. (XI. 6.) Korm. rendelet módosítása.

3.1.3 SZEÜSZ

A 79. oldal szövege az alábbiak szerint kerül módosításra:

- **Központi Kormányzati Szolgáltatás Busz:** *A KKSZB szolgáltatója biztosítja a jogszabály szerinti informatikai együttműködés biztonságos feltételeit, egyes támogató szolgáltatások elérhetőségét azon együttműködő szervek részére, amelyek megfelelnek a csatlakozás műszaki és adminisztratív feltételeinek és megállapodást kötnek a szolgáltatóval*
- **Mesterséges Intelligenciával támogatott szolgáltatások** – *a szolgáltatás lehet:*
    - *mesterséges intelligenciával támogatott hangképzés-szolgáltatás, mely az elektronikus formában rendelkezésre álló szöveget gépi úton hangalapú beszéddé történő átalakítása,*
    - *mesterséges intelligenciával támogatott hangleiratozás-szolgáltatás: mely az élő beszédet, vagy archív-mentett médiaanyagokban a digitálisan rögzített beszédet írásos szöveggé alakítja át,*
    - *mesterséges intelligenciával támogatott kommunikációs asszisztens: mely olyan szoftveres megoldás, mely öntanuló módon képes bizonyos ügyfélmegkeresések kezelésére.*
- ~~**Szerepkör tanúsítási központi platform szolgáltatás***: SZTSZ alkalmazásakor a szolgáltató biztosítja az alany számára az elektronikus dokumentumon a szerepkör tanúsítvány elhelyezését, mellyel igazolható, hogy az elektronikus dokumentum aláírása időpontjában az alany rendelkezett az aláíráshoz szükséges szerepkörrel.*~~
- ~~**Szerepkör tanúsítási szolgáltatás***: a szerepkör tanúsítvány szolgáltató az ügyintézési folyamat során az elektronikus dokumentumokon szabványos,*

~~*géppel értelmezhető, az érintettnek az eljárásban betöltött szerepkörét tanúsító rövid érvényességű tanúsítványt állít ki.*~~

- ~~**Automatikus közigazgatási döntéshozatali rendszer***: a rendszer az elektronikus ügyintézést biztosító szerv részére automatikus döntéshozatali eljárás lefolytatásának, illetve a mérlegelést igénylő ügyekben a döntési javaslat készítésének lehetőségét biztosítja.* A piaci szereplők a SZEÜSZ, KEÜSZ tartalmával azonos tartalmú, a piaci szereplők részére nyújtható központi állami szolgáltatást (a továbbiakban: PKASZ) vehetnek igénybe. A fejezetben felsorolt SZEÜSZ- és KEÜSZ-szolgáltatások jegyzéke a vonatkozó jogszabályban foglaltakkal egyezik meg. Az elektronikus közigazgatási szolgáltatások folyamatos bővülésével a szolgáltatások listája is folyamatosan bővülni fog. A központi elektronikus ügyintézési szolgáltatás igénybe vételéhez regisztráció szükséges a központi azonosítási szolgáltatással.~~

Indokolás: jogszabályváltozás, a 2023. évi CIII. törvény és a 322/2024. (XI. 6.) Korm. rendelet módosítása.

3.1.3 SZEÜSZ

A 79. oldal szövege az alábbiak szerint kerül módosításra:

~~**Elektronikus Ügyintézési Felügyelet**~~
Digitális szolgáltatások felügyelete

A digitális szolgáltatások felügyeletére a Digitális Magyarország Ügynökség Zrt. került kijelölésre. ~~A felügyelet a szolgáltatók elektronikus ügyintézéssel kapcsolatos jogszabályban foglaltaknak történő megfelelését ellenőrzi~~. A Felügyelet feladata a digitális állampolgársághoz, a digitális szolgáltatások igénybevételéhez való jog érvényesülésének, továbbá a digitális szolgáltatások biztosításának ellenőrzése, összehangolása és elősegítése.

Ezen tevékenységi körében az alábbi feladatokat végzi:

- ~~kezdeményezi a SZEÜSZ-ökre és KEÜSZ-ökre vonatkozó jogszabályok megalkotását és módosítását;~~
- ~~véleményezi az elektronikus ügyintézést érintő jogszabályokat;~~
- ~~nyilvántartja az elektronikusan intézhető ügyeket és ügyintézést biztosító szerveket;~~
- ~~ellenőrzi a SZEÜSZ-öket és KEÜSZ-öket;~~
- ~~kivizsgálja a hozzá érkezett bejelentéseket;~~
- ~~ellenőrzi az elektronikus ügyintézést biztosító szervek jogszabályban meghatározott kötelezettségeinek teljesítését;~~
- ~~vezeti az információforrások regiszterét, az adat- és iratmegnevezések jegyzékét;~~
- ~~fogadja az információátadási szabályzatok és megállapodások bejelentését;~~
- ~~műszaki irányelveket fogad el;~~
- ~~felügyeli az együttműködő szervek elektronikus ügyintézési törvényben szabályozott tevékenységeit.~~
- felügyeli a digitális szolgáltatást biztosító szervezetek által nyújtott digitális szolgáltatásokat, támogató szolgáltatásokat, digitális állampolgárság szolgáltatásokat
- életesemény-kataszterben nyilvántartja a felhasználó számára elérhető digitális szolgáltatásokat, életesemények szerint tematizált ügyeket és a digitális szolgáltatást biztosító szervezeteket;
- engedélyezi és nyilvántartásba veszi a törvény alkalmazását önként vállaló jogalanyokat;
- felhasználó bejelentése alapján felügyeleti vizsgálatot indíthat;
- hivatalból felügyeleti vizsgálatot indíthat, ha valószínűsíthető, hogy digitális szolgáltatást biztosító szervezet, a támogató szolgáltatásokat és a digitális

állampolgárság szolgáltatásokat nyújtó szervezet a törvényben meghatározott kötelezettségeit vagy a felhasználók törvényben meghatározott jogait megsérti;
- ellátja állami alkalmazásokkal és digitális szolgáltatások nyújtásával kapcsolatos követelményeket meghatározó jogszabályokban foglaltak végrehajtásának ellenőrzésével kapcsolatos hatósági és felügyeleti feladatokat és eljár azok megsértése esetén;
- kérelemre vagy hivatalból koordinációs eljárást folytat le.
- ellátja a támogató szolgáltatások és a digitális állampolgárság szolgáltatások tekintetében e szolgáltatásoknak a szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól szóló törvény szerinti hatósági felügyeletét.

Indokolás: jogszabályváltozás, a 2023. évi CIII. törvény módosítása.

3.1.3 SZEÜSZ

A 80. oldal szövege az alábbiak szerint kerül módosításra:

~~**Elektronikus ügyintézési szolgáltatás nyújtása:**~~

~~A szolgáltató köteles a felügyelet részére a szolgáltatás megkezdésére irányuló szándékát bejelenteni. Amennyiben a szolgáltatóval és a bejelentéssel kapcsolatosan kifogás nem merül fel, a felügyelet nyilvántartásba veszi a szolgáltatót. A szolgáltatás csak a nyilvántartásba vételt követően három hónappal kezdhető meg.~~

~~A szolgáltatás tervezett megszűntetését a felügyeletnek a megszűnését megelőzően legalább kilencven nappal jelezni kell.~~

Digitális szolgáltatás nyújtása

A digitális szolgáltatás nyújtását önként vállaló szervezet a digitális szolgáltatások biztosítását a digitális szolgáltatások felügyeletének engedélyével önkéntesen vállalhatja.

Az engedély kiadásának feltétele

- a Magyarország kiberbiztonságáról szóló törvényben foglalt kiberbiztonsági követelményeknek való megfelelés biztosítása, valamint kiberbiztonsági audit lefolytatása,
- a digitális állampolgárság szolgáltató által történő regisztráció
- a digitális állampolgárság szolgáltató által meghatározott szolgáltatási feltételek elfogadása,
- a digitális állampolgárság szolgáltató által meghatározott műszaki követelmények teljesítése,
- a digitális állampolgárság szolgáltató részére kormányrendeletben meghatározott mértékű szolgáltatási díj megfizetése.

Szolgáltatás megszűntetése

A szolgáltató a Felügyelet részére köteles a szolgáltatás nyújtásának megszüntetése előtt legalább 90 nappal a szolgáltatás befejezését bejelenteni. A bejelentéstől függetlenül a szolgáltató köteles a megállapodásban vállat, vagy jogszabály által előírt szolgáltatási időszakot biztosítani.

Amennyiben a szolgáltatás nyújtását nem jogszabály írja elő kötelezően, a Felügyelet jogosult a szolgáltatás megszüntetésének idejét legfeljebb 6 hónappal elhalasztani, ha a szolgáltatás nyújtásának megszüntetése a digitális szolgáltatások igénybevétele során zavarokat okozhat.

Indokolás: jogszabályváltozás, a 2023. évi CIII. törvény és a 322/2024. (XI.6.) Kormányrendelet módosítása.

3.1.5 Ügyfélkapu
A 81. oldal szövege az alábbiak szerint kerül módosításra:

~~Ügyintézés ügyfélkapun keresztül~~
~~Az ügyfélkapun keresztül a felhasználó a sikeres azonosítást – azaz felhasználónév és jelszó megadását – követően az ügyfelek számára nyújtott szolgáltatások bármelyikét szabadon igénybe veheti.~~
~~Amennyiben az ügyfél elektronikusan aláírt dokumentumot szeretne az ügyintézés folyamatába bevonni, azt technológiától függetlenül megteheti. Első lépésként az ügyfél az elektronikusan aláírt dokumentumot eljuttatja a hatóság számára. Ezt követően a hatóság a hitelesítés szolgáltató segítségével ellenőrzi, hogy az aláírás megfelelő-e. Ha a hitelesítés szolgáltató nem az adatok egyezőségét igazolja vissza, a hatóság az ügyfelet hiánypótlásra szólítja fel. Amennyiben az adatok egyezőségét igazolja vissza a hitelesítés szolgáltató, úgy az elektronikus aláírás hiteles, megkezdődhet az érdemi ügyintézés.~~

Indokolás: jogszabályváltozás, a 2023. évi CIII. törvény módosítása.

3.1.7 Digitális állampolgárság
A 83. oldal szövege az alábbiak szerint kerül módosításra:

~~3.1.7. Digitális állampolgárság~~
~~Az E-ügyintézési törvényt 2024 őszén a digitális államról szóló törvény rendelkezési váltják fel. A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény dedikált célja a digitális térben történő ügyintézés és szolgáltatások felhasználóbarát alapokra helyezése.~~
~~A törvény alapvetéseinek lényege, hogy minden a személyi adat nyilvántartásban szereplő állampolgár független digitális térben alkalmazható azonosítót kap, melynek segítségével igénybe tudja venni a számára nyújtott digitális szolgáltatásokat. A jogszabály nevesíti a digitális szolgáltatás nyújtására kötelezett szerveket.~~
~~Emellett létre hozásra kerül a digitális állampolgárság nyilvántartás – amely egy ügyfél regisztrációs nyilvántartásnak menősül –, mely az alábbi célokat szolgálja:~~
- ~~a felhasználó felhasználói profilja aktív vagy inaktív státuszával, a digitális állampolgár azonosítóval, valamint a nyilvántartásban tárolt egyéb adatokkal kapcsolatos adatszolgáltatások teljesítése,~~
- ~~a Kormány által kötelezően biztosított elektronikus azonosítási szolgáltatás kapcsán annak hiteles biztosításához és mások jogának vagy jogos érdekének védelme érdekében az érintett személy azonosításához szükséges adatok és technikai azonosítók közhiteles kezelése.~~

~~A jogszabály meghatározza az elektronikus ügyintézés módját:~~
- ~~elsődlegesen a digitális állampolgárság keretalkalmazás használatával~~
- ~~SZÜF alkalmazásával, vagy~~
- ~~a szolgáltatást biztosító szervezet által meghatározott módon.~~

~~Szintén szabályozásra kerül a szolgáltatás és az ügyfél közötti kapcsolattartás módja.~~
~~A jogszabály ezen felül rendelkezik az ügyfelek és a szolgáltató eljárás során hatályos jogairól és kötelezettségeiről is.~~
~~Emellett a SZEÜSZ-ők és KEÜSZ-ök újradefiniálásán felül bevezetésre kerül a digitális állampolgárság szolgáltatás fogalma.~~
~~A digitális állampolgárság szolgáltatások alatt az alábbiakat értjük:~~
- ~~digitális keretszolgáltatások: a digitális térben elérhető keretszolgáltatások, mint az eAzonosítás, eAláírás, ePosta, eDokumentumkezelés, eFizetés.~~
- ~~életesemény alapú szolgáltatások: a digitális szolgáltatásokat elsősorban az állampolgárok~~
  - ~~életeseményihez köthető módon kell szolgáltatni az életesemény-kataszter alapján;~~

- ~~digitális személyiadat tárca: biztosítja a felhasználó számára mind online, mind offline személyazonosító adatok, illetve valamely attribútum felhasználását köz- és magánszolgáltatások igénybevétele érdekében.~~

~~A jogszabály a digitális szolgáltatások informatikai rendszerének, azok felügyeletének, a bizalmi szolgáltatásoknak és azok felügyeletének szabályait is meghatározza.~~

Indokolás: jogszabályváltozás, a 2023. évi CIII törvény módosítása.

V. FEJEZET: ÜGYVITEL, ÜGYKEZELÉS

2. AZ ÜGYIRATKEZELÉS SZABÁLYOZÁSA

A 93. oldal második bekezdése az alábbiak szerint módosul:

Az elektronikus ügyintézés széles körű elterjedése szükségessé tette az elektronikus iratkezelés informatikai feltételrendszerének átfogó szabályozását, amely igényt tovább erősített ~~az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény hatálybalépése.~~ a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény (továbbiakban Dáptv.) hatálybalépése.

Indokolás: A 2015. évi CCXXII. törvény hatályon kívül helyezése.

2.1. AZ ÜGYIRATKEZELÉS IRÁNYÍTÁSA, FELÜGYELETE

A 94. oldalon a táblázat az alábbiak szerint módosul:

Egyedi iratkezelési szabályzat		
Szerv	**Kiadja**	**Egyetértési jogot gyakorol**
központi államigazgatási szerv	központi államigazgatási szerv	Magyar Nemzeti Levéltár vagy az illetékes szaklevéltár és a belügyminiszter*
önkormányzati hivatal	jegyző (főjegyző)	az illetékes közlevéltár vagy Budapest Főváros Levéltára és a kormányhivatal
közfeladatot ellátó egyéb szerv	közfeladatot ellátó szerv	illetékes közlevéltár
fővárosi és vármegyei kormányhivatalok	szakmai irányítást ellátó miniszter**	Magyar Nemzeti Levéltár és a belügyminiszter*
Magyar Honvédség	honvédelmi miniszter	Hadtörténelmi Levéltár és a belügyminiszter*
rendvédelmi szervek (kivéve a polgári nemzetbiztonsági szolgálatok) s	szakmai irányítást ellátó miniszter	Magyar Nemzeti Levéltár és a belügyminiszter*
bíróságok	Országos Bírósági Hivatal elnöke	Magyar Nemzeti Levéltár
ügyészség	legfőbb ügyész	Magyar Nemzeti Levéltár
közjegyzők, bírósági végrehajtók és ezek kamarái, igazságügyi szakértők, hiteles szakfordítók, büntető ügyekben közvetítői tevékenységet végző ügyvédek	igazságügyért felelős miniszter	a belügyminiszter* és a kultúráért felelős miniszter

Indokolás: az 1995. évi LXVI. törvény 10. § (2) bekezdés c. pont.

2.2. AZ IRATOK KEZELÉSÉNEK ÁLTALÁNOS KÖVETELMÉNYEI

A 97. oldalon az ötödik bekezdés az alábbiak szerint módosul:

Ha a közfeladatot ellátó szerv csak papíralapú iratokat kezel, és iratkezelési szoftvert használ, köteles biztosítani az iratkezelési szoftverben tárolt valamennyi információnak ~~az elektronikus ügyintézés részletes szabályairól szóló~~ jogszabály digitális állampolgárság egyes szabályairól szóló jogszabály[25] szerinti elektronikus dokumentumformátumban történő automatikus előállítását.

Indokolás: Az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet hatályon kívül helyezése.

3. AZ ÜGYIRATKEZELÉS FOLYAMATA

3.1. KÜLDEMÉNYEK ÁTVÉTELE

A 101. oldalon a felsorolás az alábbiak szerint módosul:

- ~~a SZEÜSZ-ként[28] biztosított elektronikus iratok kezelése szolgáltatással a szolgáltatást végző, a központi érkeztetési ügynök szolgáltatással vagy az alkalmazott iratkezelési szoftverrel a központi érkeztetési ügynök vagy az iratkezelési szoftvert használó;~~
- ~~az a hatóság, valamint kormányablak, mely az ügyfél számára ügyintézési lehetőséget biztosít más hatóságok hatáskörébe tartozó eljárásokra;~~
- ~~elektronikus ügyintézési pont útján~~.
- a SZEÜSZ-ként[28] vagy KEÜSZ-ként biztosított, egyes elektronikus iratkezelési feladatokat ellátó szolgáltatással a szolgáltatást végző, valamint a KEÜSZ-t, SZEÜSZ-t vagy az alkalmazott iratkezelési szoftvert használó természetes személy vagy a KEÜSZ-höz, SZEÜSZ-höz csatlakozott informatikai rendszer;
- a kormányablak.

Indokolás: A 335/2005. (XII. 29) Korm. rendelet alapján módosítandó.

3.2. KÜLDEMÉNYEK FELBONTÁSA

A 104. oldalon a második bekezdés az alábbiak szerint módosul:

~~A közfeladatot ellátó szerv az érkeztetést és felbontást vagy saját maga látja el, vagy ahhoz a SZEÜSZR-ben[35] meghatározott SZEÜSZ-szolgáltató szolgáltatását veheti igénybe. Ennek keretében olyan szolgáltatót is igénybe vehet a papíralapú küldemények fogadására, amely a SZEÜSZR alapján a papíralapú irat hiteles elektronikus irattá alakítását úgy nyújtja, hogy elvégzi az elektronikus másolatnak a közfeladatot ellátó szerv részére történő továbbítását is.~~

A közfeladatot ellátó szerv az érkeztetést és felbontást saját maga láthatja el, vagy ahhoz a digitális állampolgárság egyes szabályairól szóló kormányrendelet szabályozott szolgáltatást veheti igénybe. Ennek keretében olyan szolgáltatót is igénybe vehet a papíralapú küldemények fogadására, amely a digitális állampolgárság egyes szabályairól szóló kormányrendelet alapján a papír alapú irat hiteles elektronikus irattá alakítását úgy nyújtja, hogy elvégzi az elektronikus másolatnak a közfeladatot ellátó szerv részére történő továbbítását.

Indokolás: 335/2005. (XII. 29) Korm. rendelet alapján módosítandó.

3.13.3. Irattárba helyezés
A 104. oldalon a harmadik bekezdés az alábbiak szerint módosul:

Irattárba helyezés előtt az ügykezelő ismételten átvizsgálja az iratot, hogy az irattározási szabályoknak megfelel-e (például nem került-e az ügyiratok közé más ügy irata). A feleslegessé vált munkapéldányokat ~~és másolatokat~~ , másolatokat és érdemi adatot nem tartalmazó munkaanyagokat az ügyiratból ki kell emelni és a selejtezési eljárás mellőzésével meg kell semmisíteni.

Indokolás: 335/2005. (XII. 29.) Korm. rendelet 61. § (2) bekezdése alapján módosítandó.

VI. FEJEZET: ADATVÉDELMI ÉS TITKOS ÜGYIRAT KEZELÉSI ISMERETEK

1.2. INFORMÁCIÓSZABADSÁG
A 133. oldalon a szöveg az alábbiak szerint módosul:

Emellett a közérdekű, közérdekből nyilvános adatok megismerését bárki igényelheti a közfeladatot ellátó szervtől, mely kérelemre főszabály szerint 15 napon belül érdemi választ kell adni. A határidő számos esetben meghosszabbítható, erre 2025. január 1-jétől már akkor is lehetőség nyílik, ha az adatigénylés nem egyértelmű, annak pontosítása szükséges.

Indokolás: jogszabályváltozás miatt kiegészítés.

2.4. A MINŐSÍTÉSI ELJÁRÁS SZABÁLYAI
A 137. oldalon a „Feladat- és hatáskörében minősítésre jogosultak" felsorolása az alábbiak szerint módosul:

12. a Kormány tagja, a miniszterelnök politikai igazgatója, a miniszterelnök nemzetbiztonsági főtanácsadója;

Indokolás: a minősített adat védelméről szóló 2009. évi CLV. törvény módosítása.

2.5. A MINŐSÍTETT ADAT KÉSZÍTÉSE
A 139. oldal 2. bekezdése szerinti felsorolása 7. pontja és az azt követő bekezdés az alábbiak szerint módosul:

Ezeken kívül jelölni kell:
1. a készítő szerv megnevezését,
2. az iktatószámot,
3. ha az adathordozóból megállapítható, akkor a példánysorszámot és a példányszámot,
4. elektronikus minősített adat esetét kivéve az adathordozó terjedelmét,
5. a mellékletek esetén azok
a) darabszámát,
b) ha az adathordozóból megállapítható, akkor példánysorszámát,
c) ha az adathordozóból megállapítható, akkor terjedelmét és
d) az adathordozótól eltérő szintű minősítés esetén minősítési szintjét,
6. a kiadmányozás dátumát,
7. az eredeti irattári példány esetében a kiadmányozó nevét, aláírását, az általa használt hivatali bélyegző lenyomatát, *elektronikus minősített adat esetén ~~a minősített vagy minősített tanúsítványon alapuló~~ a* legalább *fokozott biztonságú elektronikus aláírását~~,~~ vagy* bélyegzőt ~~*az elektronikus bélyegzőt és az időbélyeget*~~*.*
~~*Minősített vagy minősített tanúsítványon alapuló*~~ *A legalább fokozott biztonságú elektronikus aláírással~~, elektronikus~~ vagy bélyegzővel ~~és időbélyeggel~~ ellátott minősített adat kizárólag iratkezelési szoftverrel rendelkező elektronikus adatkezelő rendszerben hozható létre.*

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

A 141. oldal első bekezdése az alábbiak szerint módosul:

A minősítőnek a döntését saját kezűleg kell aláírnia, és ellátnia a minősített adatot kezelő szerv által használt hivatali bélyegző lenyomatával. ~~vagy elektronikus aláírásával ellátnia~~. Elektronikus minősített adat esetén a jogszabály ~~minősített vagy minősített tanúsítványon alapuló~~ a legalább fokozott biztonságú elektronikus aláírás~~,~~ vagy ~~elektronikus~~ bélyegző ~~és időbélyeg~~ alkalmazását írja elő. A minősítői döntésnek arról kell szólnia, hogy a minősítő a javaslatban foglaltak alapján milyen minősítési szintre és milyen érvényességi ideig minősíti az adatot. Helytelen az a minősítői „döntés" amikor a minősítő úgy rendelkezik, hogy egyetért vagy jóváhagyja a minősítési javaslatot, hisz ez esetben a kezdeményező minősítene. Könnyű belátni, hogy a minősítési javaslattal való egyetértés nem eredményezi a minősítés megtörténtét.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

3.1. A TITKOS ÜGYKEZELŐ FOGLALKOZTATÁSÁNAK FELTÉTELEI ÉS FELADATAI
A 148. oldalon a 3.1. ponton belüli első bekezdés az alábbiak szerint módosul:

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

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

148. oldalon a 3.1. ponton belüli 4. bekezdésében a felsorolás az alábbi új esettel egészül ki:

A titkos ügykezelő feladatait a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet (a továbbiakban: NBF kormányrendelet) nevesíti. Ezek a következők:
…..
– a minősített adatot tartalmazó adathordozó **megsemmisítésének előkészítése** és az abban történő részvétel;
– az információs önrendelkezési jogról és az információszabadságról szóló törvényben szabályozott titokfelügyeleti hatósági eljárás eredményeként a nemzeti minősített adat minősítési szintje, illetve érvényességi ideje módosításának vagy a minősítés megszüntetésének rögzítése a minősített adatot tartalmazó adathordozón, az elektronikus adatállományban vagy – ha az adathordozó jellege ezt nem teszi lehetővé – a külön kísérőlapon.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

3.2. A NYILVÁNTARTÓ, A KEZELŐPONT ÉS A KÖZPONTI NYILVÁNTARTÓK
A 149. oldalon a 3.2.1. ponton belüli utolsó bekezdés az alábbiakkal egészül ki:

A titkos ügykezelő az NBF kormányrendeletben meghatározott személyi, fizikai és adminisztratív biztonsági feltételek teljesülése esetén **egyidejűleg, de egymástól elkülönítve kezelheti a nemzeti és a külföldi** minősített adatot. Erre figyelemmel azoknál a minősített adatot kezelő szerveknél, ahol egyidejűleg kezelnek nemzeti, NATO és EU minősített adatot is, szükségtelen külön Nemzeti Nyilvántartót, NATO Nyilvántartót és EU Nyilvántartót kialakítani és működtetni, hanem **egy Nyilvántartóban, de fizikailag és adminisztratívan szétválasztva külön-külön iratkezelési segédletekben** történhet a kezelésük. A tárolásukra külön biztonsági tárolóban (páncélszekrényben) vagy egyazon tárolóban, de egymástól jól elkülönítve (például a páncélszekrényben külön polcokon elhelyezve) kerülhet sor. A tárolón a benne tárolható minősített adat legmagasabb minősítési szintjét fel kell tüntetni.
Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

3.3. A MINŐSÍTETT ADATOK NYILVÁNTARTÁSI RENDSZERE
A 150. oldalon a 3.3. ponton belüli 3. bekezdés az alábbiak szerint módosul:
Az NBF kormányrendelet az alábbi iratkezelési segédleteket nevesíti:
1. az iktatókönyv nemzeti, NATO és EU minősített adatok részére külön-külön megnyitva,
2. a belső átadókönyv vagy más belső átadóokmány (például átadókarton),
~~3. a külső kézbesítőkönyv,~~
~~4.~~ 3. a futárjegyzék-nyilvántartás.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

3.3.2. Az iratkezelési segédletekre vonatkozó előírások
Az iktatókönyvre vonatkozó előírások
A 152. oldal 5. bekezdésében szereplő felsorolás az alábbiak szerint módosul:

Az NBF kormányrendelet felsorolja azokat a rovatokat, amelyeket a nemzeti minősített adatok, valamint a „Bizalmas!” vagy az annál magasabb NATO és EU minősített adatok iktatására szolgáló iktatókönyvnek minimálisan tartalmaznia kell. Ezek a következők:
1. az iktatószám,
2. az érkezés időpontja, módja,
3. az iktatás időpontja,
4. a minősítési szint és az érvényességi idő,
5. a küldő megnevezése,
6. a küldő iktatószáma (hivatkozási szám),
7. a tárgy,
~~8. az ügyintéző szervezeti egység és az ügyintéző neve,~~
~~9.~~ 8. az adathordozó papíralapú vagy elektronikus megjelenési formája és – ha az adathordozóból megállapítható – terjedelme,
~~10.~~ 9. a mellékletek darabszáma, valamint papíralapú vagy elektronikus megjelenési formája és – ha az adathordozóból megállapítható – példánysorszáma, terjedelme, valamint az adathordozótól eltérő szintű minősítés esetén minősítési szintje;
~~11.~~ 10. ha az adathordozóból megállapítható – a példánysorszám,
~~12.~~ 11. a továbbítás időpontja, módja,
~~13.~~ 12. a továbbításra kerülő példányok címzettje és – ha az adathordozóból megállapítható – példánysorszáma és terjedelme,
~~14.~~ 13. az irattárba, elektronikus minősített adat esetén az elektronikus irattárba helyezés kelte,

~~15.~~ 14. a megsemmisítés vagy a törlés időpontja, a megsemmisítési vagy törlési jegyzőkönyv
iktatószáma,
~~16.~~ 15. a felülvizsgálat dátuma és eredménye a minősítési szint csökkentése, az érvényességi idő módosítása vagy a minősítés megszüntetése esetén,
~~17.~~ 16. a kezelési bejegyzés (csatolás, határidő, visszaérkezés stb.)
2024. július 7-ig az iktatókönyvben kötelező volt az ügyintéző szervezeti egység és az ügyintéző nevét is feltüntetni, azonban ez már nem jogszabályi követelmény.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

A belső átadókönyvre vagy más belső átadó okmányra vonatkozó előírások
A 153. oldal 4. bekezdése az alábbiak szerint módosul:

A minősített adat szerven belül történő átadására és visszavételére szolgáló belső átadókönyvnek vagy átadó kartonnak tartalmaznia kell:
• a minősített adat iktatószámát,
• a minősítés szintjét,
• a példánysorszámot,
• a példányonkénti terjedelmet,
• az átadás dátumát,
• az átadás tényének igazolását az átvevő nevének és saját kezű~~, dátummal ellátott~~ aláírásának, valamint az átvétel dátumának feltüntetésével,
• a visszavétel dátumát,
• a visszavétel tényének igazolását a visszavevő nevének és saját kezű~~, dátummal ellátott~~ aláírásának, valamint a visszavétel dátumának feltüntetésével.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

A 153. oldalon az alábbi cím és azon belül az 1-2. bekezdés az alábbiak szerint változik:

A ~~külső kézbesítőkönyvre és a~~ futárjegyzékre vonatkozó előírások
A futárjegyzék a minősített adatot tartalmazó küldemény más szerv részére történő belföldi továbbítására szolgál.
~~A külső kézbesítőkönyv a minősített adatot kezelő szerv vezetője által szükség esetén kijelölt személyes kézbesítő útján történő továbbítására alkalmazható iratkezelési segédlet.~~ **2024. július 7-ig külső kézbesítőkönyvet** is lehetett alkalmazni, elsősorban a minősített adatnak a minősített adatot kezelő szerv vezetője által szükség szerint kijelölt **személyes kézbesítő útján történő szállításánál,** azonban ennek lehetősége már megszűnt, így a személyes kézbesítő útján történő szállításnál is futárjegyzéket kell használni.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

A 154. oldal 4. és 5. bekezdése az alábbiak szerint módosul:

Az NBF kormányrendelet szerint ~~a külső kézbesítőkönyvnek vagy~~ a futárjegyzéknek rendelkeznie kell az alábbi rovatokkal:
1. a minősített adat iktatószáma és példánysorszáma,
2. minősítési szint,

3. címzett,
4. az átadás kelte,
5. az átadás tényének igazolása az átvevő nevének és saját kezű aláírásának feltüntetésével, az átvétel dátuma és időpontja, továbbá a küldeményt átvevő szerv hivatalos bélyegzőjének lenyomata.
~~Ezek az iratkezelési segédletek is~~ A futárjegyzék-nyilvántartás a benne nyilvántartott futárjegyzékekkel együtt, illetve a 2024. július 07-ig használt külső kézbesítőkönyvek a lezárásukat követő 8 év megőrzési idő elteltével a levéltári törvény szabályai szerint selejtezhetők.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

3.4. A MINŐSÍTETT ADATOK NYILVÁNTARTÁSÁNAK FOLYAMATA

3.4.1. A MÁS SZERVTŐL ÉRKEZETT MINŐSÍTETT ADAT ÁTVÉTELE

A 155. oldal 3. és 4. bekezdése az alábbiak szerint módosul:

Az átvétel igazolását megelőzően a minősített küldeményt átvevő személynek ellenőriznie kell:
• a címzés alapján a minősített adatot tartalmazó küldemény átvételére való jogosultságát,
• ~~a külső kézbesítőkönyvben vagy~~ a futárjegyzéken szereplő iktatószám és példánysorszám, valamint a minősített adatot tartalmazó küldemény csomagolásán szereplő iktatószám és példánysorszám egyezését,
• a zártan érkezett küldemény csomagolásának sértetlenségét.
Az átvevő a minősített küldemény átvételét ~~a külső kézbesítőkönyvben vagy~~ a futárjegyzéken dátum és időpont (év, hó, nap, óra, perc) feltüntetése mellett, nevének olvasható feltüntetésével, saját kezű aláírásával, valamint bélyegzőlenyomattal igazolja.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

A 155. oldal 7. bekezdése az alábbiak szerint módosul:

Amennyiben a minősített adatot tartalmazó küldemény **csomagolása sérült**, az átadó jelenlétében az átvevő a küldeményt felbontja és ellenőrzi annak tartalmát. Az intézkedésről **két példányban jegyzőkönyv készül**, amelyet az átadó és az átvevő is aláír. A jegyzőkönyv egyik példánya – aláírás ellenében – az átadónak átadásra kerül, akinek intézkednie kell a sérülés körülményeinek tisztázására. A sérülés tényét az átadási okmányon – futárjegyzéken ~~vagy a külső kézbesítőkönyvben~~ – is szerepeltetni kell.

Indokolás: *a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.*

3.4.2. A minősített küldemény felbontása

A 156. oldal 1. bekezdése az alábbiak szerint módosul:

Ha a küldeményt **a titkos ügykezelő tévedésből bontja fel** – csak a felbontást követően derül ki számára, hogy erre nem volt jogosult, például nem vette észre a címzettnek szóló „Saját kezű felbontásra!” különleges kezelési utasítást – akkor erről **két példányban jegyzőkönyvet** készít. A küldeményt szabályszerűen lezárja és a jegyzőkönyv egyik példányával együtt a címzettnek soron kívül továbbítja, vagy ha ez nem lehetséges, visszajuttatja a feladónak.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

3.4.3. Az iktatás
A 156. oldalon a 3.4.3. ponton belüli 4. bekezdés az alábbiak szerint módosul:

Kivételes szabályként az NBF kormányrendelet lehetőséget ad arra, hogy a védelmi és biztonsági igazgatás központi szervénél, a rendvédelmi szerveknél, a Nemzeti Adó- és Vámhivatalnál, a Katonai Nemzetbiztonsági Szolgálatnál, a bíróságoknál az ügyészi szerveknél a különböző években, de ugyanazon ügyben keletkezett minősített adatokat egy főszámhoz tartozó alszámokon lehet nyilvántartani.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

3.4.5. A szerven belül történő átadás és visszavétel
A 158. oldal 1. bekezdése az alábbiak szerint módosul:

A titkos ügykezelő közreműködése nélkül jogszerűen csak az ügyeleti szolgálat, illetve az őrszolgálat tagjai részére adható át a minősített adat a szolgálatátadáskor. A minősített adat szignálásra történő bemutatására is speciális szabály vonatkozik. Ha a szignálásra történő bemutatás során a minősített adat a titkos ügykezelő ~~személyes~~ felügyelete alatt marad, akkor nem szükséges annak a belső átadókönyvben vagy más átadó okmányon dokumentált módon történő átadása és visszavétele. A titkos ügykezelő közreműködése nélkül történhet az elektronikus adatkezelő rendszeren belül az elektronikus minősített adat átadása is a felhasználók között.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

3.4.6. Más szerv részére történő továbbítás belföldön
A 158. oldalon a 3.4.6. ponton belüli 2., 5. és 6. bekezdések az alábbiak szerint módosulnak:

….
A továbbításra ~~**külső kézbesítőkönyvben vagy**~~ **futárjegyzéken dokumentáltan** kerülhet sor. A titkos ügykezelő a továbbítás tényét az iktatókönyvben rögzíti.
…….
A szállítás és kézbesítés céljából a titkos ügykezelő a ~~külső kézbesítőkönyvvel vagy~~ futárjegyzékkel együtt **átadja a lezárt és a lezárás helyén a minősített adatot kezelő szerv hivatalos bélyegzőjével ellátott küldeményt a személyes kézbesítőnek vagy a futárnak**.
A szállítást követően a személyes kézbesítő (vagy a futár) ~~a külső kézbesítőkönyvben vagy~~ a futárjegyzéken **aláírás ellenében adja át a küldeményt a külső szervnél átvételre jogosult személynek.**

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.

3.5.3. A munkapéldányokra vonatkozó szabályok
A 161. oldalon a 3.5.3. pont szövege az alábbiak szerint módosul:

Az NBF kormányrendelet nem tartalmaz eljárásrendet a készítés során feleslegessé vált, nem kiadmányozott – alapvetően a papíralapú – munkapéldányok (a továbbiakban: munkapéldány) kezelésével és megsemmisítésével kapcsolatosan, de azt rögzíti, hogy a minősített adatot kezelő szerv vezetőjének **saját hatáskörben a biztonsági szabályzatban** kell rendelkeznie a munkapéldányok kezelésével és megsemmisítéséről.

Eszerint akár úgy is rendelkezhet, hogy a munkapéldányokat a többespéldányokra előírt megsemmisítési eljárás keretében kell megsemmisíteni, de úgy is dönthet, hogy ez mellőzhető, és a készítő köteles gondoskodni a munkapéldányok megsemmisítéséről. Ettől eltérően az elektronikus minősített adatok kiadmányozás előtti, feleslegessé vált munkapéldányainak törlésére az NBF kormányrendelet a felhasználónál kezelt, ügyviteli érdeket nem képviselő elektronikus példányok törlésére vonatkozó, a 3.5.2. pontban ismertetett szabályok alkalmazását írja elő.

Indokolás: a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet módosítása.