MAGYAR POSTA ZRT.

EKOP-1.2.23-2012-2012-0001 Hibrid Kézbesítési és Konverziós Rendszer

Jogszabályi összefoglaló

Magyar Posta

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Regionális Fejlesztési Alap

BEFEKTETÉS A JÖVŐBE

Az EKOP-1.2.23-2012-2012-0001 Hibrid Kézbesítési és Konverziós Rendszer kiemelt projekt során figyelembe vett legfontosabb jogszabályok kivonata

Összefoglaló lezárva: 2018. január 31.

2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól 5

466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról 18

451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól 24

137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről 60

84/2012. (IV. 21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről 67

2012. évi CLIX. törvény a postai szolgáltatásokról 71

335/2012. (XII. 4.) Korm. rendelet a postai szolgáltatások nyújtásának és a hivatalos iratokkal kapcsolatos postai szolgáltatás részletes szabályairól, valamint a postai szolgáltatók általános szerződési feltételeiről és a postai szolgáltatásból kizárt vagy feltételesen szállítható küldeményekről 73

9/2005. (I. 19.) Korm. rendelet a postai szolgáltatók, a postai közreműködők és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének részletes szabályairól 82

2016. évi CXXX. törvény a polgári perrendtartásról 88

2017. évi I. törvény a közigazgatási perrendtartásról 99

2016. évi CL. törvény az általános közigazgatási rendtartásról 100

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről 103

1998. évi XIX. törvény a büntetőeljárásról 110

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről 114

335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről 116

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 125

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról 139

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 151

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről 152

2016/679 EURÓPAI PARLAMENT ÉS TANÁCS RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) 208

910/2014/EU európai parlamenti és tanácsi rendelet a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről 233

2015/1505 BIZOTTSÁG (EU) VÉGREHAJTÁSI HATÁROZATA a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 22. cikkének (5) bekezdése szerinti bizalmi listákhoz kapcsolódó technikai specifikációk és formátumok meghatározásáról 248

2015/1506 BIZOTTSÁG (EU) VÉGREHAJTÁSI HATÁROZATA a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 27. cikkének (5) bekezdése és 37. cikkének (5) bekezdése szerint a közigazgatási szervek által elismert fokozott biztonságú elektronikus aláírások és fokozott biztonságú bélyegzők formátumaira vonatkozó specifikációk meghatározásáról 250

A jelen listában a hibrid kézbesítési és konverziós szolgáltatásokhoz kapcsolódó legfontosabb jogszabályok szerepelnek, mintegy figyelemfelhívásként. Nem vállalkozhattunk egyrészt a teljes jogi környezet bemutatására, hiszen a kapcsolat mibenléte nem definiálható pontosan. A jelen gyűjtés során a tartalmi összefüggést, a Hibrid kézbesítési és konverziós rendszer működésének meghatározásában játszott szerepet tekintettük elsődlegesnek. A jogszabályok többségét nem idéztük teljes egészében, hiszen jellemzően nem a teljes jogszabály releváns a hibrid szolgáltatások szempontjából. Jelen dokumentum a 2018. január 31. napján hatályos jogszabály szövegeket tartalmazza.

2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól

http://njt.hu/cgi_bin/njt_doc.cgi?docid=193173.337609

1. § E törvény alkalmazásában

11. *biztonságos kézbesítési szolgáltatás:* olyan kézbesítési szolgáltatás, amely az elektronikus küldemény kézbesítésével kapcsolatosan az alábbi feltételek mindegyikének teljesülését biztosítja:

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;

18. *Elektronikus Ügyintézési Felügyelet* (a továbbiakban: Felügyelet): az elektronikus ügyintézés előmozdításáért, az elektronikus ügyintézés felügyeletéért, az együttműködő szervek együttműködéséért és koordinációjáért felelős, e törvényben és a törvény végrehajtására kiadott kormányrendeletben meghatározott feladatokat ellátó, Kormány által kijelölt szerv;

20. *érvényesítési adat:* az eIDAS Rendelet 3. cikk 40. pontja szerinti adat;

21. *érvényességi lánc:* az elektronikus dokumentum vagy annak lenyomata és azon egymáshoz rendelhető információk (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás vagy bélyegző létrehozásához használt adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényességi adatára és annak visszavonására vonatkozó információk) sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, az aláírás, bélyegző vagy időbélyegző elhelyezésének időpontjában érvényes volt;

22. *fokozott biztonságú elektronikus aláírás:* az eIDAS Rendelet 3. cikkének 11. pontja szerinti aláírás;

34. *lenyomat:* olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti az e törvény végrehajtására kiadott rendeletben megfogalmazott követelményeket;

43. *tanúsítvány alany:* a tanúsítványban a bizalmi szolgáltató által igazolt azonosságú vagy tulajdonságú személy, így különösen elektronikus aláírás tanúsítványa esetén az aláíró;

44. *tanúsítvány:* az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a weboldal-hitelesítő tanúsítvány, valamint mindazon, a bizalmi szolgáltatás keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen;

6. Átjárás a papír alapú és az elektronikus ügyintézés között

12. § (1) Az elektronikus ügyintézést biztosító szerv elektronikus ügyintézése során szükség szerint

a) a papír alapon beérkező iratról hiteles elektronikus másolatot készít vagy készíttet,
b) az elektronikus úton kiadmányozott döntésről hiteles papír alapú másolatot készít vagy azt hiteles papír alapú irattá alakíttatja.

(2) Az elektronikus dokumentum bizonyító ereje megegyezik az eredeti papír alapú dokumentum bizonyító erejével

a) a papír alapú dokumentumokról elektronikus úton történő másolat készítésének szabályai szerinti hiteles másolatkészítés esetén,
b) az elektronikus irat hiteles papír alapú irattá alakítása szabályai szerinti hiteles másolatkészítés esetén.

(3) A dokumentum bizonyító ereje megegyezik az eredeti elektronikus dokumentum bizonyító erejével, ha az elektronikus irat hiteles papír alapú irattá alakítása, valamint elektronikus iratról hiteles, más formátumú elektronikus másolat készítésére irányuló központi elektronikus ügyintézési szolgáltatás szabályai szerinti készítették.

18. Szabályozott elektronikus ügyintézési szolgáltatások

29. § (1) Szabályozott elektronikus ügyintézési szolgáltatás

a) az elektronikus azonosítási szolgáltatás,
b) a biztonságos kézbesítési szolgáltatás,
c) az elektronikus ügyintézési szolgáltatások nyújtására felhasználható, jogszabályban meghatározott követelményeknek megfelelő elektronikus aláírással kapcsolatos szolgáltatás,
d) az e törvény felhatalmazása alapján kiadott kormányrendeletben szabályozott elektronikus ügyintézési szolgáltatásként nevesített szolgáltatás.

(2) Több szabályozott elektronikus ügyintézési szolgáltatás egységesen is kialakítható és nyújtható, de ez esetben is mindegyik szabályozott elektronikus ügyintézési szolgáltatásra vonatkozó követelménynek külön-külön kell a szolgáltatás nyújtójának megfelelnie.

(3) A szabályozott elektronikus ügyintézési szolgáltatások bejelentésére, a szabályozott elektronikus ügyintézési szolgáltatások nyilvántartásának vezetésére, a Felügyelet tevékenységére vonatkozó, valamint a szabályozott elektronikus ügyintézési szolgáltatások nyújtásának részletes szabályait a Kormány rendelete határozza meg. A szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól szóló törvény rendelkezései a jelen alcím szerinti, valamint a Kormány rendeletében meghatározott eltérésekkel megfelelően alkalmazandók.

(4) Törvény vagy kormányrendelet szabályozott elektronikus ügyintézési szolgáltatás igénybevételét kötelezővé teheti.

20. A Kormány által kötelezően biztosítandó szabályozott elektronikus ügyintézési szolgáltatások

34. § (1) Az alábbi szabályozott elektronikus ügyintézési szolgáltatásokat a Kormány köteles biztosítani, a kijelölt szabályozott elektronikus ügyintézési szolgáltató útján:

a) elektronikus azonosítási szolgáltatás természetes személy ügyfelek részére,

b) biztonságos kézbesítési szolgáltatás,

c) kormányzati hitelesítés-szolgáltatás, ezen belül az alábbi szolgáltatások:

ca) elektronikus ügyintézési szolgáltatások nyújtására felhasználható, jogszabályban meghatározott követelményeknek megfelelő elektronikus aláírással, elektronikus bélyegzővel kapcsolatos szolgáltatások nyújtása, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, az elektronikus ügyintézést biztosító szervek, valamint az e törvény szerinti szabályozott elektronikus ügyintézési szolgáltatók és központi elektronikus ügyintézési szolgáltatók általi felhasználás céljára,

cb) elektronikus időbélyegzőkkel kapcsolatos szolgáltatások nyújtása, valamint azonosítási célú tanúsítvány szolgáltatás az elektronikus ügyintézést biztosító szervek, valamint az e törvény szerinti szabályozott elektronikus ügyintézési szolgáltatók és központi elektronikus ügyintézési szolgáltatók általi felhasználás céljára,

cc) elektronikus aláírással, elektronikus bélyegzővel kapcsolatos szolgáltatások nyújtása, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása külön jogszabályban meghatározott védelem alá eső tisztséget betöltő, valamint nemzetbiztonsági ellenőrzés alá eső jogviszonyban álló személyek, titkos információgyűjtés, valamint titkos adatszerzés eszközei és módszerei alkalmazásában, engedélyezésében részt vevő szervek részére,

cd) titkosítási célú tanúsítványok kibocsátása az elektronikus ügyintézést biztosító szervek, az e törvény szerinti szabályozott elektronikus ügyintézési szolgáltatók és központi

elektronikus ügyintézési szolgáltatók általi felhasználás céljára, külön jogszabályban meghatározott védelem alá eső tisztséget betöltő, valamint nemzetbiztonsági ellenőrzés alá eső jogviszonyban álló személyek részére,

ce) a *ca)-cd)* alpontok szerint kibocsátott tanúsítványok érvényességének igazolása azonnali tanúsítványállapot-igazoló szolgáltatással,

d) az e törvény felhatalmazása alapján kiadott kormányrendeletben kötelezően nyújtandóként előírt további szabályozott elektronikus ügyintézési szolgáltatás.

(2) Jogszabály az (1) bekezdésben foglaltakon túl egyes szabályozott elektronikus ügyintézési szolgáltatások nyújtását más szervek számára is előírhatja.

22. Adatkezelés

36. § (1) A szabályozott elektronikus ügyintézési szolgáltatónak úgy kell megválasztania és minden esetben oly módon kell üzemeltetnie a szolgáltatás nyújtása során alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez feltétlenül szükséges, azonban ebben az esetben is csak a szükséges mértékben és ideig.

(2) A szabályozott elektronikus ügyintézési szolgáltató a 34. § (1) bekezdés *a)-c)* pontjai szerinti szabályozott elektronikus ügyintézési szolgáltatás nyújtására irányuló szerződés létrehozása, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, ahol szükséges, az abból származó díjak számlázása, valamint az azzal kapcsolatos követelések érvényesítése céljából kezelheti az igénybe vevő azonosításához szükséges természetes személyazonosító adatokat és lakcímet.

(3) A (2) bekezdésben foglaltakon túl a szabályozott elektronikus ügyintézési szolgáltató a szabályozott elektronikus ügyintézési szolgáltatás nyújtására irányuló szerződésből származó díjak számlázása céljából kezelheti a szabályozott elektronikus ügyintézési szolgáltatás igénybevételével kapcsolatos természetes személyazonosító adatokat, lakcímet, valamint a szolgáltatás igénybevételének időpontjára, időtartamára és helyére vonatkozó adatokat.

(4) A szabályozott elektronikus ügyintézési szolgáltató a szabályozott elektronikus ügyintézési szolgáltatás nyújtása céljából kezelheti azon személyes adatokat, amelyek a szolgáltatás nyújtásához technikailag elengedhetetlenül szükségesek.

(5) A (2)-(3) bekezdésben meghatározott célokból kezelt adatokat a szerződés létrejöttének elmaradását követően haladéktalanul, a szerződés megszűnése esetén pedig a megszűnéstől számított 5 év elteltével kell törölni. A (4) bekezdésben meghatározott célból kezelt adatokat haladéktalanul törölni kell, ha az adatkezelési cél megszűnt.

(6) Ahol a szolgáltatás keretében adatfeldolgozás valósul meg, a szolgáltatási szerződést oly módon kell megkötni, hogy a szerződés tartalma a személyes adatok tekintetében kielégítse az

információs önrendelkezési jogról és az információszabadságról szóló törvény által az adatfeldolgozás vonatkozásában meghatározott feltételeket.

37. § (1) A szabályozott elektronikus ügyintézési szolgáltató a szabályozott elektronikus ügyintézési szolgáltatás alkalmazásával elektronikus ügyintézést biztosító szerv megkeresésére - a szolgáltatás igénybe vevője azonosító adatainak ellenőrzése céljából - adategyeztetést végez, és az adatok egyezéséről vagy az eltérés tényéről a megkereső elektronikus ügyintézést biztosító szervet tájékoztatja.

(2) A szabályozott elektronikus ügyintézési szolgáltatónak biztosítania kell, hogy az igénybe vevő a szolgáltatás igénybevétele előtt és az igénybevétel során bármikor megismerhesse, hogy a szabályozott elektronikus ügyintézési szolgáltató mely adatkezelési célokból mely adatfajtákat kezel.

(3) A szabályozott elektronikus ügyintézési szolgáltató a szabályozott elektronikus ügyintézési szolgáltatás nyújtása során kezelt személyes adatot, üzleti titkot, banktitkot, fizetési titkot, biztosítási titkot, értékpapírtitkot, pénztártitkot, orvosi titkot és más hivatás gyakorlásához kötött titkot kizárólag továbbított információként, közbenső és átmeneti jelleggel tárolhatja. A szolgáltatás teljesítését követően az adatokat köteles az elektronikus információs rendszereiből és adathordozóiról haladéktalanul törölni.

(4) A szabályozott elektronikus ügyintézési szolgáltató alkalmazottait az (1) bekezdés szerint megismert adatok tekintetében titoktartási kötelezettség terheli, amely a foglalkoztatásra irányuló jogviszony megszűnését követően is fennmarad.

VII. FEJEZET
KÖZPONTI ELEKTRONIKUS ÜGYINTÉZÉSI SZOLGÁLTATÁSOK

38. § (1) Az alábbi központi elektronikus ügyintézési szolgáltatásokat a Kormány biztosítja a jogszabályban kijelölt szolgáltató útján:

a) az ügyfél ügyintézési rendelkezésének nyilvántartása,

b) iratérvényességi nyilvántartás,

c) elektronikus fizetési és elszámolási rendszer,

d) azonosításra visszavezetett dokumentumhitelesítés,

e) központi érkeztetési ügynök, amelynek keretében a szolgáltató az elektronikus ügyintézést biztosító szerv javára ellátja a részére elektronikus úton érkezett küldemények átvétele, felbontása és érkeztetése tekintetében kormányrendeletben meghatározott feladatokat,

f) központi kézbesítési ügynök, amelynek keretében a szolgáltató az elektronikus ügyintézést biztosító szerv javára ellátja az általa kiküldendő elektronikus iratok kézbesítésének előkészítése, adathordozójának, fajtájának meghatározása, továbbá a kézbesítés módja tekintetében a kormányrendeletben meghatározott feladatokat,

g) az ügyfél időszaki értesítése az elektronikus ügyintézési cselekményekről, amelynek keretében a szolgáltató az ügyfelet az általa meghatározott elektronikus ügyintézést biztosító

szervek tekintetében és időszakonként összesítve tájékoztatja a kormányrendeletben meghatározott ügyintézési cselekményekről,

h) papír alapú irat átalakítása hiteles elektronikus irattá,

i) elektronikus irat hiteles papír alapú irattá alakítása,

j) központi azonosítási ügynök,

k) személyre szabott ügyintézési felület,

l) űrlapbenyújtás-támogatási szolgáltatás,

m) központi dokumentumhitelesítési ügynök,

n) általános célú elektronikus kéreleműrlap szolgáltatás,

o) összerendelési nyilvántartás.

(2) Amennyiben a központi elektronikus ügyintézési szolgáltatás igénybevételéhez regisztráció szükséges, a regisztrációra jogszabály eltérő rendelkezése hiányában kizárólag elektronikus azonosítási szolgáltatással kerülhet sor. A regisztráció során az elektronikus azonosítási szolgáltató az igénybe vevő hozzájárulása alapján jogosult a kijelölt szolgáltató részére átadni a regisztrációhoz szükséges, az elektronikus azonosítási szolgáltató által kezelt személyes adatokat.

(3) Törvény vagy kormányrendelet valamely központi elektronikus ügyintézési szolgáltatás igénybevételét kötelezővé teheti.

(4) A Kormány által kijelölt szolgáltató központi elektronikus ügyintézési szolgáltatás nyújtásával összefüggő adatkezelése körében a 36. § és a 37. § rendelkezései megfelelően alkalmazandóak.

23. Az ügyfél ügyintézési rendelkezésének nyilvántartása

39. § (1) A Kormány által kijelölt szerv az elektronikus ügyintézés megkönnyítése, az ügyfél választási lehetőségeinek megteremtése és elektronikus ügyintézéssel kapcsolatos rendelkezésének tiszteletben tartása érdekében az ügyfél ügyintézési rendelkezéseinek adattartamáról nyilvántartást vezet.

(2) Az összerendelési nyilvántartás adatkezelője új természetes személy összerendelési bejegyzésének nyilvántartásba történő bejegyzésekor elektronikus úton értesíti az ügyfél ügyintézési rendelkezését nyilvántartó szervet abból a célból, hogy a személy rendelkezéseinek kezelése céljából a személy számára rendelkezési nyilvántartási bejegyzést hozzon létre.

(3) A rendelkezési nyilvántartást vezető szerv a (2) bekezdés szerint átadott természetes személyazonosító adatok alapján a személy részére belső azonosítót és összerendelési bejegyzési kapcsolati kódot képez, majd gondoskodik az összerendelési bejegyzési kapcsolati kód titkosított változatának - csak általa visszafejthető titkosítással - az összerendelési nyilvántartást vezető szerv részére történő továbbításáról, ezt követően a természetes személyazonosító adatokat törli.

(4) A rendelkezési nyilvántartást vezető szerv a képviseletre vonatkozó rendelkezés nyilvántartásba vétele során a képviselőt az összerendelési nyilvántartáson alapuló szolgáltatás

igénybevételével veszi nyilvántartásba, a képviselő természetes személyazonosító adatait és a más hatóság által képzett azonosítót vagy azonosító kódot nem tárolja.

(5) A rendelkezési nyilvántartást vezető szerv a képviseleti jogosultságot megvizsgálja.

(6) A rendelkezési nyilvántartást vezető szerv az ügyfél által tett nyilatkozatot titkosítva tárolja, azt az ügyfélen kívül kizárólag jogszabály felhatalmazása vagy az ügyfél ügyintézési rendelkezése alapján, az arra jogosult személynek bocsátja rendelkezésre.

(7) Az ügyfél ügyintézési rendelkezésének tartalmáról a rendelkezési nyilvántartást vezető szerv az arra jogosult szervet vagy személyt - az összerendelési nyilvántartáson alapuló szolgáltatás igénybevételével - jogszabályban meghatározott módon tájékoztatja, ha a szerv vagy személy megadja az ügyfél azonosításához szükséges adatokat. A rendelkezési nyilvántartást vezető szerv az arra jogosult szervet vagy személyt csak az ügyfél azon ügyintézési rendelkezésének tartalmáról tájékoztatja, amelyet jogszabály számára lehetővé tesz, vagy az ügyfél az ügyintézési rendelkezése szerint az adott szervvel vagy személlyel meg kívánt osztani.

(8) A rendelkezési nyilvántartást vezető szerv kizárólag az elektronikus ügyintézést biztosító szervek vagy szabályozott elektronikus ügyintézési szolgáltatás, illetve központi elektronikus ügyintézési szolgáltatás szolgáltató számára szolgáltat adatot az ügyintézési rendelkezés tartalmáról, ideértve az ügyfél által adott meghatalmazás adatait is. Az elektronikus ügyintézést biztosító szervek vagy más, szabályozott elektronikus ügyintézési szolgáltatás, illetve központi elektronikus ügyintézési szolgáltatás szolgáltató igazolja, hogy mely azonosító kódok, illetve más azonosítók használatára jogosult.

(9) Az ügyintézési rendelkezés tartalmáról történő tájékoztatás során a nyilvántartó szerv az összerendelési nyilvántartás igénybevételével kizárólag olyan azonosító kódot vagy más adatot közölhet a megkereső szervvel, szolgáltatóval, amelynek kezelésére az érintett szerv vagy szolgáltató jogosult.

(10) Törvény vagy kormányrendelet lehetővé teheti, hogy az elektronikus ügyintézést biztosító szerv, a szabályozott vagy a központi elektronikus ügyintézési szolgáltatás szolgáltatója az ügyfél jogszabályban meghatározott egyes ügyintézési rendelkezéseit, jogszabályban meghatározott módon a rendelkezési nyilvántartást vezető szervnek nyilvántartásba vétel céljából bejelentse.

(11) A rendelkezési nyilvántartást kezelő szerv vagy a rendelkezési nyilvántartás regisztrációs szerve az ügyfél vagy más szerv vagy a (10) bekezdés szerinti szolgáltató által az ügyintézési rendelkezés nyilvántartásba vétele során megadott személyes adatokat - ha törvény eltérően nem rendelkezik - kizárólag a rendelkezés nyilvántartásba vétele céljából, annak nyilvántartásba rögzítése idejéig kezeli.

24. Iratérvényességi nyilvántartás

40. § (1) Az iratérvényességi nyilvántartás szolgáltatás keretében a szolgáltató lehetővé teszi, hogy az igénybe vevő a birtokában lévő hiteles papír alapú vagy elektronikus okiratok hitelességét, illetve - amennyiben erre adatok rendelkezésre állnak - tartalmát ellenőrizze.

(2) Az iratérvényességi nyilvántartás szolgáltatás igénybe vevője az iratérvényességi nyilvántartásban rögzíti az általa kiállított okiratoknak a szolgáltató által meghatározott egyes adatait, illetve tartalmi elemeit. Az iratérvényességi nyilvántartás nyilvánosan elérhető, abban bárki ellenőrizheti a birtokában lévő, a nyilvántartásban rögzített okiratnak a nyilvántartásban elérhető adatait, valamint adott esetben az okirat hitelességét is.

25. Papír alapú irat átalakítása hiteles elektronikus irattá

41. § Az iratról a papír alapú irat átalakítása hiteles elektronikus irattá szolgáltatás szabályai szerint a Kormány által kijelölt szerv által készített okirat bizonyító ereje megegyezik az eredeti okiratéval.

26. Elektronikus irat hiteles papír alapú irattá alakítása

42. § Az elektronikus iratról az elektronikus irat hiteles papír alapú irattá alakítása szolgáltatás szabályai szerint a Kormány által kijelölt szerv által készített okirat bizonyító ereje megegyezik az eredeti okiratéval.

VII/A. FEJEZET
EGYES E-ÜGYINTÉZÉSI SZOLGÁLTATÁSOK IGÉNYBEVÉTELE

42/A. § A törvényben vagy kormányrendeletben meghatározott szabályozott elektronikus ügyintézési szolgáltatások és központi elektronikus ügyintézési szolgáltatások - a Kormány rendeletében meghatározott módon - az elektronikus ügyintézést nem biztosító szerv által is igénybevehető.

IX. FEJEZET
AZ ELEKTRONIKUS ÜGYINTÉZÉS FELÜGYELETE

46. § (1) A Kormány által rendeletben kijelölt Felügyelet ellátja az elektronikus ügyintézést biztosító szervek e Részben meghatározott kötelezettségei teljesítésének felügyeletét és elősegíti az ügyfelek e Részben meghatározott jogainak érvényesülését.

(2) Az elektronikus ügyintézést biztosító szerv kérelmére a Felügyelet közreműködik az elektronikus ügyintézés biztosításához szükséges intézkedések koordinációjában.

(3) A Felügyelet a szabályozott és a központi elektronikus ügyintézési szolgáltatások tekintetében ellátja e szolgáltatásoknak a szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól szóló törvény szerinti hatósági felügyeletét.

(4) A Felügyelet a felügyeleti vizsgálat során a központi vagy szabályozott elektronikus ügyintézési szolgáltatások jogszabályban meghatározott követelményeinek megtartását hatósági ellenőrzés keretében vizsgálja.

(5) Ha a Felügyelet megállapítja, hogy a központi vagy szabályozott elektronikus ügyintézési szolgáltatások szolgáltatója e törvényben vagy az e törvény végrehajtási rendeleteiben foglalt szabályokat megsértette,

a) kötelezi a szolgáltatót a jogsértés abbahagyására és a jogszerű eljárásra,
b) szükség szerint határidő tűzésével kötelezheti a szolgáltatót a jövőre nézve a jogszerű eljárásra,
c) a Kormány által rendeletben meghatározott mértékű bírságot szabhat ki.

29. Koordinációs eljárás

49. § (1) A Felügyelet az elektronikus ügyintézést biztosító szerv kérelmére vagy hivatalból koordinációs eljárást folytat le. A koordinációs eljárás célja az elektronikus ügyintézés kialakításának, valamint módosításának e törvényben foglaltak szerinti megvalósítása.

(2) A koordinációs eljárás során a Felügyelet:

a) szakmai segítséget nyújt az elektronikus ügyintézés kialakításában, módosításában,
b) konzultációt folytat le a szabályozott elektronikus ügyintézési szolgáltató, valamint az elektronikus ügyintézést biztosító szerv részvételével,
c) javaslatot tehet meghatározott szolgáltatás, megoldás alkalmazására.

XI. FEJEZET
EGYÜTTMŰKÖDŐ SZERVEK KÖZÖTTI ELEKTRONIKUS KAPCSOLATTARTÁS

59. § (1) Ha a kézbesítéshez jogszabály nem fűz jogkövetkezményt, valamint tájékoztatás céljából az együttműködő szervek biztonságos elektronikus kapcsolattartásnak nem minősülő módon is tarthatják elektronikus úton egymással a kapcsolatot.

(2) Az együttműködés kialakítása, valamint belső folyamatai biztosítása érdekében az együttműködő szerv a Második Rész szerinti szabályozott elektronikus ügyintézési szolgáltatásokat és a központi elektronikus ügyintézési szolgáltatásokat igénybe veheti.

(3) Az együttműködő szerv az e törvény szerinti együttműködés során szükség szerint a csak papír alapon rendelkezésre álló iratról e törvény szabályai szerinti hiteles elektronikus másolatot

készít vagy - az elektronikus ügyintézésről szóló törvény szerinti központi elektronikus ügyintézési szolgáltatás igénybevételével - készíttet.

XIV. FEJEZET
EGYÜTTMŰKÖDÉS SORÁN HASZNÁLT SZABÁLYOZOTT ÉS KÖZPONTI ELEKTRONIKUS ÜGYINTÉZÉSI SZOLGÁLTATÁSOK

74. § (1) Az együttműködés elősegítése érdekében az együttműködő szerv az együttműködés során, valamint a belső elektronikus ügymenete során a VI. és VII. Fejezetben, valamint e törvény végrehajtási rendeletében meghatározott szabályozott és központi elektronikus ügyintézési szolgáltatásokat igénybe veheti.

(2) Az (1) bekezdés szerinti igénybevétel során a VI. és VII. Fejezetben meghatározott szabályokat értelemszerűen, az adatkezelésére vonatkozó szabályok betartásával kell alkalmazni.

(3) A 38. §-ban meghatározott szolgáltatásokon túl az alábbi központi elektronikus ügyintézési szolgáltatásokat a Kormány biztosítja a jogszabályban kijelölt szolgáltató útján:

a) központi érkeztetési rendszer, amely biztosítja az iratkezelés egyes fázisainak központi szolgáltatás útján történő elvégzését,

b) elektronikus dokumentumtárolás szolgáltatás, amely biztosítja a szolgáltatás keretében tárolt elektronikus dokumentum hitelességének megőrzését, tartós olvashatóságát és értelmezhetőségét,

c) iratkezelő rendszerek közötti iratáthelyezés szolgáltatás, amely biztosítja az együttműködő szervek között elektronikus iktatókönyvben nyilvántartott irat vagy irategyüttes dokumentált átadását,

d) központi kormányzati szolgáltatás busz, amelynek keretében

da) a szolgáltató az együttműködő szervek, valamint a szolgáltatáshoz önkéntesen csatlakozott egyéb szervezetek információs rendszereinek automatikus információátadási felületei csatlakoztatásával, ennek hiányában információátadási szolgáltatásként biztosítja az egymás közötti automatikus információátadás biztonságos feltételeit, valamint

db) a csatlakozott együttműködő szervek személyes adatokat tartalmazó információs rendszereinek adattovábbítási nyilvántartásai vonatkozásában - az információs önrendelkezési jogról és az információszabadságról szóló törvény alapján - az érintett személyes adatainak továbbítására vonatkozó tájékoztatásadást támogató egyablakos, tájékoztatási szolgáltatást biztosít.

(4) Törvény vagy kormányrendelet valamely központi elektronikus ügyintézési szolgáltatás igénybevételét az együttműködés során is kötelezővé teheti.

(5) A Kormány az együttműködéshez, valamint a belső elektronikus ügymenethez szükséges szabályozott elektronikus ügyintézési szolgáltatásokat és központi elektronikus ügyintézési szolgáltatásokat az 1. § 17. pont *a)-i)* pontja szerinti jogalanyoknak ingyenesen biztosítja.

60. Felhatalmazó rendelkezések

105. § (1) Felhatalmazást kap a Kormány, hogy rendeletben állapítsa meg

a) az elektronikus ügyintézés és az elektronikus kapcsolattartás részletes szabályait,

b) az elektronikus ügyintézési szolgáltatásnak és a központi elektronikus ügyintézési szolgáltatásnak az elektronikus ügyintézést nem biztosító szerv által történő felhasználása feltételeit, a felhasználás során a Felügyelet feladatát és eljárását, valamint a szolgáltatás használatáért számítható díj megállapításának módját,

c) a szabályozott elektronikus ügyintézési szolgáltatások és a központi elektronikus ügyintézési szolgáltatások részletes követelményeit, a szolgáltatásnyújtás részletes eljárási rendjét, a szolgáltatás igénybevételének részletes szabályait, a szabályozott elektronikus ügyintézési szolgáltatásnyújtásra vonatkozó szervezési és a szolgáltató által teljesítendő személyi és pénzügyi feltételeket, a szabályozott elektronikus ügyintézési szolgáltatás bejelentésével, valamint a Felügyelet általi bírság kiszabásával kapcsolatos rendelkezéseket és a bírság mértékét,

d) az elektronikus ügyintézést biztosító szerv azonosításával kapcsolatos részletes követelményeket,

e) az elektronikus kapcsolattartási módokra vonatkozó részletes szabályokat,

f) az ügyintézési rendelkezés tételének és nyilvántartásba vételének részletes szabályait,

g) az elektronikus ügyintézés céljaira felhasználható elektronikus aláírásokra, az elektronikus aláíráshoz tartozó tanúsítványokra, illetve az azokkal összefüggésben nyújtott elektronikus aláírással kapcsolatos szolgáltatásokra vonatkozó sajátos követelményeket,

h) az elektronikus ügyintézési szolgáltató regisztrációjának részletes szabályait,

i) az összerendelési nyilvántartás működésének és az összerendelési nyilvántartásból történő adatszolgáltatás nyújtásának részletes szabályait,

j) az elektronikus fizetésekre és elszámolásokra vonatkozó részletes szabályokat,

k) a Felügyelet eljárásának részletes szabályait,

l) a 14. § (7) bekezdése szerinti jogalanyok körét,

m) az országos telefonos ügyfélszolgálat működésének részletes szabályait,

n) a papír alapú dokumentumokról elektronikus úton történő másolat készítésére vonatkozó részletes szabályokat,

o) az elektronikus ügyintézést biztosító szerveknek az ügyek intézésével kapcsolatos adatai biztonsági mentésének rendjét és gyakoriságát, valamint az adatok őrzéséért felelős szervet,

p) a bizalmi felügyelet által vezetett nyilvántartás tartalmával és a bizalmi szolgáltatás nyújtásával összefüggő bejelentésekkel kapcsolatos követelményeket.

(2) Felhatalmazást kap a Kormány, hogy rendeletben jelölje ki

a) a Felügyeletet,

b) az elektronikus ügyintézést igénybe vevő külföldi személyek nyilvántartását vezető szervet,

c) a Kormány által kötelezően biztosított szabályozott elektronikus ügyintézési szolgáltatások

szolgáltatóit, valamint a központi elektronikus ügyintézési szolgáltatások szolgáltatóit,

d) a Központi Ügyfél-regisztrációs Nyilvántartást vezető szervet, valamint a Kormány által kötelezően biztosított elektronikus azonosítási szolgáltatás és a rendelkezési nyilvántartás regisztrációs szerveit,

e) az országos telefonos ügyfélszolgálatot működtető szervet.

(3) Felhatalmazást kap a Kormány, hogy rendeletben állapítsa meg

a) az informatikai együttműködést biztosító szolgáltatások rendelkezésre állására és annak igazolására vonatkozó szabályokat,

b) az együttműködő szervek közzétételi kötelezettségei teljesítésére szolgáló közzétételi felületre vonatkozó szabályokat,

c) az informatikai együttműködést korlátozó vagy akadályozó üzemszünet és üzemzavar esetén követendő eljárásra vonatkozó részletes szabályokat,

d) a műszaki irányelvek elfogadására és közzétételére vonatkozó részletes szabályokat,

e) az automatikus információátadásra köteles együttműködő szerveket és az ilyen módon továbbítandó információk körét, valamint az automatikus információátadási felületre vonatkozó követelményeket,

f) az információátadási szabályzat részletes tartalmi követelményeit, valamint az információátadási szabályzatban szabályozandó információk körét,

g) az információátadási szabályzat és megállapodás bejelentésére vonatkozó szabályokat,

h) az információforrások regisztere adattartalmára és vezetésére vonatkozó részletes szabályokat,

i) az adat- és iratmegnevezések jegyzéke adattartalmára és vezetésére vonatkozó részletes szabályokat,

j) a központi címregiszter vezetése, működése, az egységes címképzés szabályait, valamint az egységes címkezelés részletes eljárási szabályait,

k) az e törvény szerinti központi elektronikus ügyintézési szolgáltatásokra vonatkozó szabályokat, a kötelezően igénybe veendő központi elektronikus ügyintézési szolgáltatások körét,

l) a 104. § (1) bekezdés szerinti informatikai fejlesztési tervre, valamint bejelentésre és a bejelentés jogkövetkezményeire vonatkozó részletes szabályokat,

m) a felügyeleti vizsgálat részletes szabályait, valamint

n) a koordinációs eljárás részletes szabályait.

(4) Felhatalmazást kap a Kormány, hogy az

a) elektronikus kapcsolattartásra vonatkozó elérhetőségek,

b) elsődleges információforrásból rendelkezésre álló információk

e törvényben nem szabályozott típusait, körét rendeletben határozza meg.

(5) Felhatalmazást kap a Kormány, hogy rendeletben jelölje ki

a) a központi címregiszter működtetéséért felelős szervet,
b) a Harmadik Rész szerinti együttműködésre kijelölt közfeladatot ellátó szerveket, valamint
c) a 104. § (1) bekezdése szerinti szervet.

(5a) Felhatalmazást kap a Kormány, hogy rendeletben határozza meg

a) az önhibán kívüli akadályozottság hatálya alatt álló elektronikus ügyintézést biztosító szerveket,
b) azon, az *a)* pont szerinti szerv feladat- és hatáskörébe tartozó ügyeket, amelyek esetében az önhibán kívüli akadályozottság nem áll fenn, és
c) az önhibán kívüli akadályozottság időtartamát.

(6) Felhatalmazást kap az e-közigazgatásért felelős miniszter, hogy az adópolitikáért felelős miniszterrel egyetértésben a szabályozott elektronikus ügyintézési szolgáltatások bejelentéséért, a szabályozott elektronikus ügyintézési szolgáltatásokat érintő változások bejelentésért fizetendő igazgatási szolgáltatási díj mértékét, a díj megfizetésével, kezelésével, nyilvántartásával kapcsolatos szabályokat rendeletben állapítsa meg.

106. § Felhatalmazást kap az e-közigazgatásért felelős miniszter, hogy

a) a bizalmi szolgáltatásokkal kapcsolatos részletes követelményeket, így különösen a bizalmi szolgáltatók pénzügyi és személyzeti megfelelőségével, a tevékenységével és az általa használt eszközökkel kapcsolatos követelményeket, az igénybe vevők szerződésének megkötésével és a szerződéskötéssel összefüggő tájékoztatási kötelezettségével kapcsolatos követelményeket, valamint a szolgáltatási szerződésre, a bizalmi szolgáltatás nyújtásának egyéb feltételeire (így a bizalmi szolgáltatási rendre és szolgáltatási szabályzatra) vonatkozó részletes feltételeket,
c) az adópolitikáért felelős miniszterrel egyetértésben a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékét, valamint a díj megfizetésével, kezelésével, nyilvántartásával, visszatérítésével kapcsolatos részletes szabályokat,
d) a 104/A. § (1) bekezdés *a)* pontja alapján a központi szolgáltató által fejlesztett vagy üzemeltetett informatikai rendszert, valamint a nem a Kormány irányítása vagy felügyelete alá tartozó költségvetési szerv által igénybevett központosított informatikai és hírközlési szolgáltatásokat

rendeletben állapítsa meg.

466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=206247.349832

1. Értelmező rendelkezések

1. § E rendelet alkalmazásában

1. *adattrezor-archiválás:* az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési tv.) 25. § (4a) bekezdése szerinti, az elektronikus ügyintézést biztosító szervnek az ügyek intézésével kapcsolatos, elektronikus információs rendszereiben és nyilvántartásaiban tárolt nem minősített adatai biztonsági mentése;

2. *Felügyelet:* az E-ügyintézési tv. 1. § 18. pontjában meghatározott Elektronikus Ügyintézési Felügyelet;

3. *kisméretű archív állomány:* az adattrezor-archiválás mérete az adatokkal és a teljes futtatási környezettel együtt nem éri el a 300 megabájtot;

4. *Kormányzati Adattrezor:* olyan kormányzati adatbank, amely az adattrezor-archivált állományokat fogadja és biztonságosan tárolja, őrzi, és az adatok adatkezelő részére történő kiadásával újraépíthetővé teszi a különböző informatikai rendszereket;

6. *NISZ Zrt.:* a NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság;

8. *teljes futtatási környezet:* a számítógépen alkalmazott programok futtatásához szükséges szoftverkörnyezet, melynek részét képezi az operációs rendszer, a telepített programkönyvtárak, segédprogramok, rendszerbeállítások.

2. Az adatkezelő

2. § (1) Az adattrezor-archiválási kötelezettség az e-ügyintézést biztosító szervet, továbbá a központi elektronikus ügyintézési szolgáltatást, valamint szabályozott elektronikus ügyintézési szolgáltatást nyújtó szervet (a továbbiakban együtt: adatkezelő) terheli az általa saját szoftverkörnyezetben kezelt adatok tekintetében. Ha az adatkezelő szerződés alapján adatfeldolgozót vesz igénybe, az adatfeldolgozással érintett adatok tekintetében az adattrezor-archiválást és az ahhoz kapcsolódó, e rendeletben meghatározott feladatokat az adatkezelő az adatfeldolgozó útján látja el.

(2) Az adatkezelő felelőssége, hogy az archivált adatokból az eredeti környezet teljes vagy részleges megsemmisülése esetén helyreállítható legyen az eredeti működés a megfelelő hardvereszközök üzembe helyezését követően.

3. Az őrzésért felelős szerv

3. § (1) A Kormány az adattrezor-archiválások Kormányzati Adattrezorban történő őrzéséért és az adattrezor-archiválási rendszer üzemeltetéséért felelős szervként (a továbbiakban együtt: őrzésért felelős szerv) a NISZ Zrt.-t jelöli ki.

(2) Az őrzésért felelős szerv feladata adatfeldolgozóként az adattrezor-archiválás átvétele, biztonságos és szakszerű tárolása és visszaszolgáltatása, valamint az adattrezor-archiválási rendszer üzemeltetése.

4. Az adattrezor-archiválás tartalma, átadása, megőrzése

4. § (1) Az adattrezor-archiválási kötelezettség célja az adatkezelőnek az e-ügyintézési kötelezettség teljesítésével összefüggő adatai sérüléséből eredő működési zavara esetén a működési képesség helyreállítása és az adatvesztés minimalizálása.

(2) Az adattrezor-archiválást olyan formátumban kell elvégezni, hogy abból értelmezhető adatot csak az adatkezelő, és csak az archiválás visszaállítását követően tudjon előállítani.

(3) Ha az archiválási kötelezettséggel érintett nyilvántartások esetén az adatok visszaállítása aránytalanul költséges vagy időigényes, az adattrezor-archiválás az adatokkal együtt a teljes futtatási környezet archiválását is tartalmazza.

(4) Az adattrezor-archiválás a legutolsó állapot helyreállításához szükséges adatállományokat tartalmazza. Az adatkezelő és az őrzésért felelős szerv megállapodhat abban, hogy az adattrezor-archiválás időállapotokat is tartalmaz.

(5) Első alkalommal valamennyi elektronikus információs rendszer vagy nyilvántartás esetében a teljes adatállományt archiválni kell. A változások archiválása ehhez az állományhoz képest történik úgy, hogy a legutolsó állomány legfeljebb két állományból helyreállítható legyen. A teljes adatállomány archiválása esetén az archiválandó adatmennyiség őrzésért felelős szerv részére történő átadása az adatkezelő által biztosított fizikai adathordozó használatával történik. Az adatkezelő és az őrzésért felelős szerv megállapodhat abban, hogy a technikai és biztonsági feltételek fennállása esetén a teljes adatállomány átadása hálózati kapcsolat útján történjen.

(6) Az elektronikus információbiztonságra vonatkozó szabályokból következő biztonsági mentési kötelezettség nem váltható ki az adattrezor-archiválási kötelezettséggel.

5. § (1) Az adattrezor-archiváláshoz szükséges, az adatkezelő archiválási rendszere és az adattrezor központi megoldása közötti egységes formátumot biztosító virtuális eszközrendszert az őrzésért felelős szerv bocsátja az adatkezelő rendelkezésére. Az adatkezelő az archiváláshoz - a nemzetbiztonsági szolgálatok elektronikus információs rendszerei adattrezor-archiválását kivéve - ezt az eszközrendszert köteles használni. A virtuális eszközrendszer rosszindulatú szoftverkódoktól való mentességéért az őrzésért felelős szerv a felelős.

(2) A virtuális eszközrendszert futtató infrastruktúrát az adatkezelő biztosítja. A 13. § (3) bekezdésében meghatározott adatmennyiséget meghaladó kapacitásigény esetén az egységes formátumot biztosító eszközrendszert az őrzésért felelős szerv fizikai úton biztosítja.

(3) Az adattrezor-archiválást titkosító kulcs alkalmazásával az adatkezelőnek úgy kell elvégeznie, hogy abból az adatkezelőnél működtetett elektronikus információs rendszerek külön-külön is visszaállíthatóak legyenek. Az adatkezelőnek jól beazonosítható módon meg kell jelölnie, hogy az átadott adatállomány mely adatkezelő elektronikus információs rendszere archiválását tartalmazza. Az adattrezor-archiválásnak tartalmaznia kell a visszaállításhoz szükséges dokumentációt.

(4) Az őrzésért felelős szervnek átadásra kerülő adatállománynak a technika archiváláskori állása szerint rosszindulatú szoftverkódtól való mentessége az adatkezelő szerv felelőssége.

6. § (1) Az adattrezor-archiváláshoz szükséges titkosító kulcsot az Információs Hivatal állítja elő két példányban, és egy példányt eljuttat az adatkezelőhöz. Valamennyi adatkezelő szervet saját, egyéni kulccsal kell ellátni. A kulcs nem hozható harmadik szerv vagy személy tudomására, csak az adatkezelőnek vagy jogutódjának, vagy törvényben kijelölt szervnek adható ki. Az Információs Hivatal által átadott kulcsról az adatkezelő másolatot készít és azt biztonságos helyen tárolja.

(2) Az Információs Hivatal elkülönítetten tárolja a titkosító kulcs egy példányát, és azt az adatkezelő vagy jogutódja rendelkezésére bocsátja, ha az adatkezelőnél lévő titkosító kulcs és annak másolata megsemmisül, vagy mindkettő megsérül.

7. § (1) A titkosított adattrezor-archiválás átadása - az őrzésért felelős szerv és az adatkezelő szerződése alapján, a 9. § szerinti kivétellel - történhet

a) az archivált adatállományokat tartalmazó fizikai adattároló eszköz rendelkezésre bocsátásával vagy
b) hálózati kapcsolat útján.

(2) Ha az adattrezor-archiválás mérete miatt az adattrezor-archiválás átadása aránytalan terhet ró az adatkezelőre, az adattrezor-archiválás átadása az adatkezelő által biztosított fizikai adattároló eszköz rendelkezésre bocsátásával történik.

(3) Ha az adattrezor-archiválás átadása fizikai adattároló eszköz rendelkezésre bocsátásával történik, az adattároló eszközt az adatkezelő által kijelölt személy adja át az őrzésért felelős szerv által kijelölt személynek. A kijelölt személynek a személyazonosságát és a kijelölés tényét igazolnia kell.

(4) Ha az adattrezor-archiválás átadása fizikai adattároló eszköz rendelkezésre bocsátásával történik, az eszközt az őrzésért felelős szerv az azonos archiválási gyakoriságú adattrezor-archiválás következő átadásakor az adatkezelőnek visszaadja.

8. § Az adattrezor-archiválás megőrzése - a 9. § szerinti kivétellel - történhet

a) ha van, a fizikai adattároló eszköz helyreállíthatatlan módon történő törlése vagy az eszköz adatkezelőnek történő visszaadása mellett az archív állomány központi tárolóhelyre történő, logikai elkülönítést biztosító másolásával vagy

b) az átadott fizikai adattároló eszköz tárolásával.

9. § (1) Kisméretű archív állomány esetén az adattrezor-archiválás

a) átadása hálózati kapcsolat útján,

b) megőrzése az archív adatállomány központi tárolóhelyre történő, logikai elkülönítést biztosító másolásával történik.

(2) A nemzetbiztonsági szolgálatok hatósági feladatokhoz kapcsolódó, minősített adatot nem tartalmazó elektronikus információs rendszerei esetében az adattrezor-archiválás

a) átadását kizárólag az adatkezelő által biztosított fizikai adattároló eszköz alkalmazásával lehet végrehajtani,

b) megőrzése az átadott fizikai adattároló eszköz tárolásával történik.

10. § Hálózati kapcsolat útján történő adattrezor-archiválás esetén a hálózati kapcsolat meglétének biztosítása az adatkezelő, a biztonságos hálózati kapcsolat kiépítése az őrzésért felelős szerv és az adatkezelő együttes felelőssége.

6. Archiválási kategóriába sorolás

12. § (1) Az adattrezor-archiválásra kötelezett adatkezelő archiválási szabályzatot készít (a továbbiakban: archiválási szabályzat). Az archiválási szabályzat az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti informatikai biztonsági szabályzat részeként is elkészíthető.

(2) Az archiválási szabályzat tartalmazza az adatkezelőnek az elektronikus ügyintézés biztosításához szükséges elektronikus információs rendszerei

a) megnevezését,

b) által tárolt adatok körét,

c) e rendelet szerinti archiválási kategóriába sorolását,

d) vonatkozásában annak megjelölését, hogy csak egyes adatok vagy azzal együtt a teljes futtatási környezet archiválására van-e szükség.

(3) Az adatkezelőnek az elektronikus ügyintézés biztosításához szükséges elektronikus információs rendszereit az 1. melléklet szerinti archiválási kategóriába kell besorolnia, archiválásukat az ott meghatározott gyakorisággal kell elvégeznie.

(4) Az archiválási szabályzatot, a benne foglalt információk változása esetén, a változást követő 3 napon belül frissíteni kell.

(5) Az archiválási szabályzatot annak elkészítésekor, valamit módosításakor a Felügyeletnek meg kell küldeni. A Felügyelet az archiválási szabályzat beérkezését követő 60 napon belül az archiválási szabályzatot felülvizsgálja, és álláspontjáról az adatkezelőt értesíti.

(6) A Felügyelet az archiválási szabályzatokról belső használatú katalógust vezet.

(7) Az archiválási szabályzat Felügyeletnek történő megküldésével egyidejűleg el kell kezdeni az adattrezor-archiválás végrehajtását.

(8) Ha a Felügyelet az archiválási szabályzat 12. § (2) bekezdés *b)* vagy *c)* pontja szerinti tartalmával nem ért egyet, az adatkezelőt annak módosítására kötelezi. Ebben az esetben az adatkezelő - a módosított tartalom szerinti archiválási kategóriába sorolásnak megfelelően - ismételten adattrezor-archiválást végez.

7. Az adattrezor-archiválás felügyelete

13. § (1) Az E-ügyintézési tv. 78. §-ában meghatározott hatáskörében a Felügyelet műszaki irányelvet ad ki, mely tartalmazza az archív állományokat tároló központi tárolóhelyre, a fizikai adattároló eszközök formátumára és tárolására, valamint a hálózati kapcsolat útján történő átadásra vonatkozó műszaki és biztonsági javaslatokat.

(2) Az (1) bekezdés szerinti műszaki irányelv elkészítésébe a Felügyelet az őrzésért felelős szervet bevonja.

(3) Az őrzésért felelős szerv - a Felügyelet útján - közzéteszi azt a maximális, egy adatkezelőre jutó adatmennyiséget, mely esetében az adattrezor-archiváláshoz szükséges, az adatkezelő archiválási rendszere és az adattrezor központi megoldása közötti egységes formátumot biztosító eszközrendszer virtuális úton kerül biztosításra.

14. § (1) A Felügyelet - éves ellenőrzési terv alapján, valamint szükség esetén azon túl is - az adattrezor-archiválási kötelezettség végrehajtását az adatkezelőnél ellenőrzi. Ennek keretében az adattrezor-archiválásból - előzetes bejelentési kötelezettség mellett - próba-visszaállítást rendelhet el. A próba-visszaállítás végrehajtásakor figyelemmel kell lenni arra, hogy az ne eredményezzen aránytalan mértékű szolgáltatáskiesést, valamint ne veszélyeztesse az érintett elektronikus információs rendszer működését. A próba-visszaállítás sikeres, ha a szervezet működésében zavar nem keletkezik, és az adatterzor-archiválásban foglalt valamennyi adat hiánytalanul és hibamentesen visszaállításra kerül. Erről a szervezet vezetője nyilatkozik.

(2) A próba-visszaállítás célja annak megállapítása, hogy az elektronikus ügyintézés tekintetében történt-e sérülés.

A próba-visszaállítás során a Felügyelet a visszaállított adatokat nem ellenőrizheti, azokat nem ismerheti meg.

(3) A Felügyelet - a jogsértés mértékétől függően -

a) az archiválási szabályzat elkészítésének vagy módosításának elmulasztása esetén tízezertől

ötszázezer forintig terjedő,

b) az adattrezor-archiválási kötelezettség megsértése esetén ötszázezertől ötmillió forintig terjedő bírságot szabhat ki.

1. melléklet a 466/2017. (XII. 28.) Korm. rendelethez

Archiválási kategóriák

	A	B	C
1	Kategória	Az adott kategóriába tartozó elektronikus információs rendszer vagy nyilvántartás	Archiválási gyakoriság és adatok köre
2	1. kategória - kiemelt rendszerek	1. A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendeletben meghatározott nyilvántartások. 2. Az E-ügyintézési tv. szerinti központi elektronikus ügyintézési szolgáltatások, valamint szabályozott elektronikus ügyintézési szolgáltatások működését biztosító elektronikus információs rendszerek és nyilvántartások, az E-ügyintézési tv. 42/A. §-ában foglalt szervek által történő igénybevételhez kapcsolódó nyilvántartások kivételével.	- első alkalommal, valamint legalább havonta teljes állomány archiválása - naponta változások archiválása (kisméretű archív állomány esetén minden esetben teljes állomány archiválása)
3	2. kategória	Az elektronikus ügyintézést biztosító szerv naponta frissülő elektronikus információs rendszerei és nyilvántartásai, amelyek 1 héten túli kiesése az elektronikus ügyintézést biztosító szerv E-ügyintézési tv. 25. § (3) bekezdése szerinti kötelességei ellehetetlenülését okozza.	- első alkalommal, valamint legalább háromhavonta teljes állomány archiválása - naponta változások archiválása (kisméretű archív állomány esetén minden esetben teljes állomány archiválása)
4	3. kategória	Az elektronikus ügyintézést biztosító szerv naponta frissülő elektronikus információs rendszerei és nyilvántartásai, amelyek 1 hónapon túli kiesése az elektronikus ügyintézést biztosító szerv E-ügyintézési tv. 25. § (3) bekezdése szerinti kötelességei ellehetetlenülését okozza.	- első alkalommal, valamint legalább félévente teljes állomány archiválása - havonta változások archiválása (kisméretű archív állomány esetén minden esetben teljes állomány archiválása)
5	4. kategória	Az elektronikus ügyintézést biztosító szerv legfeljebb átlagosan hetente frissülő elektronikus információs rendszerei és nyilvántartásai, amelyek 6 hónapon túli kiesése az elektronikus ügyintézést biztosító szerv E-ügyintézési tv. 25. § (3) bekezdése szerinti kötelességei ellehetetlenülését okozza.	- első alkalommal, valamint legalább félévente teljes állomány archiválása
6	5. kategória	1. Az 1-4. kategóriába nem sorolható, az E-ügyintézési tv.-ben meghatározott kötelezettségek teljesítésével összefüggő elektronikus információs rendszerek és nyilvántartások. 2. A *a)* bírósági végrehajtó, az önálló bírósági végrehajtó iroda, *b)* hegyközségek kivételével a köztestület, *c)* törvényben vagy kormányrendeletben elektronikus ügyintézésre kötelezett közfeladatot ellátó vagy közszolgáltatást nyújtó jogalany elektronikus információs rendszerei és nyilvántartásai.	- első alkalommal, valamint legalább évente teljes állomány archiválása

451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól

http://njt.hu/cgi_bin/njt_doc.cgi?docid=199341.346972

1. A rendelet hatálya

1. § (1) A rendelet hatálya - a (2) és (3) bekezdésben foglalt kivétellel - az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési tv.) szerinti elektronikus ügyintézésre, az annak során eljáró szervezetekre és ügyfeleikre, a szabályozott elektronikus ügyintézési szolgáltatások és a központi elektronikus ügyintézési szolgáltatások nyújtóira és igénybe vevőire, valamint az elektronikus ügyintézést biztosító szervek és más szervek közötti informatikai együttműködésre terjed ki.

(2) A III. Fejezet hatálya a papíralapú közokiratról, papíralapú magánokiratról és papíralapú számviteli bizonylatról történő elektronikus másolat készítésére, az annak során eljáró személyekre terjed ki.

(3) A 23/A. alcím hatálya az E-ügyintézési tv. szerinti szabályozott elektronikus ügyintézési szolgáltatások és a központi elektronikus ügyintézési szolgáltatások nyújtóira és azok E-ügyintézési tv. 42/A. § szerinti igénybevevőire, valamint az Elektronikus Ügyintézési Felügyeletre terjed ki.

2. § E rendelet alkalmazásában:

1. *digitalizálás:* olyan eljárás, amely az analóg felépítésű információt számítástechnikai eszközök számára feldolgozható, digitális információvá alakítja át;

2. *elektronikus űrlap:* minden olyan elektronikus formában adatszolgáltatásra szolgáló felület, amelynél a megadandó adatok formája és tartalmi köre előre rögzített, és a kitöltést követően a megadott tartalommal elektronikus dokumentum jön létre;

3. *folytonos védelem:* az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelem;

4. *hiteles elektronikus másolat:* valamely nem elektronikus dokumentumról e rendelet szabályai szerint készült, azzal képileg vagy tartalmilag egyező, joghatás kiváltására alkalmas elektronikus eszköz útján értelmezhető adategyüttes;

5. *képi megfelelés:* az elektronikus másolat azon tulajdonsága, amely biztosítja a papíralapú dokumentum - joghatás kiváltása szempontjából lényeges - tartalmi és formai elemeinek megismerhetőségét;

6. *kockázattal arányos védelem:* olyan védelem, mely biztosítja, hogy egy kellően nagy időintervallumban a védelem költségei arányosak legyenek a potenciális kárértékkel;

7. *másolatkészítő rendszer:* a másolatkészítés során alkalmazott hardver, szoftver, valamint ezek együttese;

8. *nyilvános kulcsú infrastruktúra:* kriptográfiai kulcspárral működő informatikai rendszertechnológia, amelynek működési elve, hogy ha egy elektronikus adatot, illetve dokumentumot a megadott kulcspár egyik kulcsának segítségével átalakítanak, akkor azt csak az adott kulcspár másik kulcs tagjával lehet az eredeti állapotába visszaállítani;

9. *rendelkezésre állás:* az elektronikus információs rendszerek az arra jogosult személyek számára történő elérhetőségének és az abban kezelt adatok felhasználhatóságának az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti biztosítása;

10. *rendelkezésre állás célértéke:* a rendelkezésre állási követelményhez rendelt, számmal és mértékegységgel meghatározott, az elektronikus ügyintézést biztosító szerv által vállalt, kötelezően teljesítendő érték;

11. *tartalmi megfelelés:* az elektronikus másolat azon tulajdonsága, amely szerint az − a hozzá kapcsolódó metaadatokkal együttesen − biztosítja a papíralapú dokumentum − a joghatás kiváltása szempontjából lényeges − tartalmi elemeinek megismerhetőségét, de nem biztosítja a képi megfelelést;

12. *teljes körű védelem:* a rendszer valamennyi elemére kiterjedő védelem;

13. *visszavonási állapotinformáció szolgáltatás:* hiteles, visszavonási állapotinformációkat tartalmazó szolgáltatás;

14. *zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem;

15. *zárt rendszer:* rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja, működése jogszabályon vagy meghatározott résztvevők közötti megállapodáson alapul, és harmadik felet nem érint;

6. § (5) Ha az ügyben az E-ügyintézési tv. alapján elektronikus ügyintézésre köteles és nem köteles ügyfél is részt vesz, az elektronikus ügyintézést biztosító szerv köteles digitalizálni a papír alapon keletkezett iratokat az elektronikus ügyintézésre köteles félnek történő továbbításuk érdekében.

(6) Az (5) bekezdés szerinti esetben az elektronikus ügyintézést biztosító szerv köteles az elektronikusan keletkezett iratokról hiteles papíralapú másolatot készíteni vagy készíttetni, ha az az elektronikus ügyintézésre nem köteles ügyfélnek történő kézbesítésük érdekében, az ügyfél kérelmére vagy más okból szükséges.

(7) Ha a papír alapon keletkezett iratok elektronikus továbbítása szükséges elektronikus ügyintézést biztosító szervek között, a digitalizálásról az az elektronikus ügyintézést biztosító szerv köteles gondoskodni, amelynek eljárása során az irat keletkezett.

(8) A digitalizálást vagy az elektronikus iratról hiteles papíralapú másolat készítését az elektronikus ügyintézést biztosító szervnek 5 - különösen nagy mennyiségű irat esetén 10 - munkanapon belül kell elvégeznie, kivéve, ha az ügy intézési határideje ennél rövidebb.

7. Dokumentumhitelesítés

12. § (1) Hiteles az elektronikus dokumentum, ha

a) az teljes bizonyító erejű magánokiratnak minősül, és - ha jogszabály így rendelkezik - időbélyegzővel látták el,

b) a nyilatkozattevő vagy kiállító elektronikus ügyintézést biztosító szerv - illetve annak nevében kiadmányozásra jogosultjának - legalább fokozott biztonságú elektronikus aláírásával vagy bélyegzőjével és - ha jogszabály így rendelkezik - időbélyegzővel látták el,

c) iratérvényességi nyilvántartásban elhelyezték,

d) az aláíró vagy kiadmányozásra jogosult azt az azonosításra visszavezetett dokumentumhitelesítés szolgáltatással hitelesítette,

e) kizárólag az elektronikus ügyintézést biztosító szerv zárt informatikai rendszerében történő felhasználás esetén a szerv zárt informatikai rendszerében rögzítették, vagy

f) jogszabályban meghatározott más módon hitelesítették.

(2) Az (1) bekezdés szerint hitelesített elektronikus dokumentumba foglalt nyilatkozatról vélelmezni kell, hogy az a megtétele óta változatlan.

(3) Az E-ügyintézési tv. 21/A. § (4) bekezdése szerinti esetben az ügyfél a beadványát digitalizálja, és azt az (1) bekezdés *a)* és *d)* pontja szerint hitelesíti.

(4) Az (1) bekezdés *b)-f)* pontja szerint hiteles irat akkor közokirat, ha megfelel a törvényben meghatározott, a közokiratra vonatkozó további feltételeknek.

(5) Törvény az (1) bekezdés *b)* pontjában foglalt esetben minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást vagy bélyegzőt is megkövetelhet.

13. § (1) Ha a dokumentum az iratérvényességi nyilvántartásban szerepel, úgy a másolat és az iratérvényességi nyilvántartásban elhelyezett elektronikus dokumentum egyezése és az elektronikus dokumentum hitelessége akkor állapítható meg, ha

a) az elektronikus irat egyezése megállapítható az iratérvényességi nyilvántartásban elhelyezett elektronikus dokumentummal,

b) a papíralapú irat tartalmi egyezése megállapítható az iratérvényességi nyilvántartásban elhelyezett elektronikus dokumentummal a képi megjelenés alapján.

(2) Zárt rendszerben azonosítás alapján feljegyzett hitelesítési adat vagy hozzárendelés alapján létrehozott elektronikus dokumentum akkor tekinthető hitelesnek, ha az informatikai biztonságra vonatkozó előírásoknak megfelelően auditálással igazolt

a) a rendszer zártsága,

b) az azonosítás alapján történő hozzárendelés megfelelősége, valamint

c) a hitelességi információk megváltoztatása észlelhető.

(3) A (2) bekezdés szerinti zárt rendszerben hitelesnek tekintett dokumentumok zárt rendszeren kívüli felhasználását az elektronikus ügyintézést biztosító szerv a hitelesmásolat-készítés szabályai szerint készített másolattal teszi lehetővé.

14. § (1) Az elektronikus ügyintézést biztosító szerv a 12. § (1) bekezdés *a)* pontja szerinti követelmények teljesülése hiányában is hitelesnek fogadhatja el az ügyfél más elektronikus ügyintézést biztosító szerv előtt tett nyilatkozatát vagy más elektronikus ügyintézést biztosító szerv által tárolt adatot, ha a másik elektronikus ügyintézést biztosító szerv igazolja, hogy

a) a nyilatkozat megtételére, az adat rögzítésére az ügyfél azonosítását követően került sor,

b) a nyilatkozat vagy adat zárt rendszerben került tárolásra úgy, hogy a nyilatkozat, illetve adat megváltoztatása észlelhető.

(2) Az elektronikus ügyintézést biztosító szervek közötti adatkapcsolat és az annak keretében továbbított adat vagy dokumentum a 12. § (1) bekezdés *e)* pontja szerinti követelmények teljesülése hiányában is hitelesnek fogadható el, ha

a) az adattovábbítás automatikus információátadási felületének biztosítása olyan zárt rendszerek között történik, ahol a továbbított adat a zárt rendszeren belül mind az információ átadását biztosító szerv, mind az információt átvevő szerv oldalán hitelesként kezelt, vagy

b) jogszabály az elektronikus ügyintézést biztosító szervek és az adatok vagy dokumentumok megjelölésével kifejezetten így rendelkezik.

15. § (1) Zárt rendszer esetében hitelesnek kell tekinteni a dokumentumot, ha az a zárt rendszerben jön létre és kizárólag - harmadik felet nem érintve - a zárt rendszerben kerül kezelésre.

(2) Az (1) bekezdés szerinti dokumentum zárt rendszeren kívüli hitelesítéséhez a 12. § (1) bekezdés szerinti hitelesítése szükséges.

16. § A 12. § (3) bekezdésében foglalt eset kivételével, valamint ha jogszabály eltérően nem rendelkezik, több nyilatkozattevő nyilatkozatát tartalmazó dokumentum akkor tekinthető hitelesnek, ha a 12. és 13. § rendelkezéseinek alkalmazásával azt valamennyi nyilatkozattevő hitelesítette, vagy azt valamennyi nyilatkozattevő tekintetében hitelesítették.

8. Beadványok formátumai

17. § (1) Az elektronikus ügyintézést biztosító szerv az ebben az alcímben foglalt rendelkezések és a rá vonatkozó jogszabályok alapján határozza meg, hogy - az 1. mellékletben meghatározott, kötelezően elfogadandó - formátumokon túlmenően az elektronikus kapcsolattartás keretében milyen formátumú elektronikus dokumentumokat fogad el.

(2) Az elektronikus ügyintézést biztosító szerv az elektronikus tájékoztatás szabályai szerint elektronikus úton közzéteszi az (1) bekezdés szerinti fájlformátumokat.

(3) Az elektronikus ügyintézést biztosító szerv a (2) bekezdés szerint közzétett formátumoktól eltérő dokumentumformátumot is elfogadhat az ügyféllel kötött megállapodása alapján, az abban meghatározott feltételekkel. Az elektronikus ügyintézést biztosító szerv a megállapodásban igényelheti a megállapodás szerinti egyedi formátum elfogadásával járó költségek megtérítését.

(4) Ha jogszabály eltérően nem rendelkezik, az elektronikus ügyintézést biztosító szerv olyan formátumú dokumentumokat küld az ügyfél részére, amelyeket az ügyfél ingyenesen bárki számára elektronikusan elérhető program segítségével olvasni tud. Az elektronikus ügyintézést biztosító szerv ettől eltérő formátumban is küldhet az ügyfélnek dokumentumot, ha az ügyféllel ebben megállapodott.

18. § Az elektronikus ügyintézést biztosító szerv megtagadhatja az olyan elektronikus dokumentum elfogadását, amely aktív vagy változó adattartalmat tartalmaz. Az elektronikus ügyintézést biztosító szerv az ilyen dokumentumot akkor fogadhatja el, ha

a) az elektronikus iratról hiteles, más formátumú elektronikus másolat készítésére vonatkozó jogszabályi rendelkezések szerint annak változó tartalmat nem tartalmazó dokumentummá alakításáról gondoskodik,
b) az adott eljárástípusban ez nincs kizárva,
c) a változó tartalom az ügy szempontjából releváns adatot nem tartalmaz, és
d) szükség esetén az ügyintézéshez szükséges mértékben, a felhasználására vonatkozó megállapításairól hivatalos feljegyzést készít.

11. Másolatok felhasználása

28. § (1) Ha az elektronikus ügyintézést biztosító szerv az iratot hiteles papíralapú másolatként kézbesíti, és a másolatkészítésre szolgáltatót vesz igénybe, akkor

a) az ügyintézési határidő számítása szempontjából a hiteles papíralapú másolat postára adásának az időpontja irányadó,
b) a döntés akkor minősül kézbesítettnek, amikor a hiteles papíralapú másolat kézbesítésre kerül, vagy azt jogszabály alapján kézbesítettnek kell tekinteni.

(2) Ha az elektronikus ügyintézés során egyes eljárási cselekmények teljesítéséhez elektronikus iratot az ügyfél rendelkezése vagy jogszabály alapján nem lehet felhasználni, és az adott elektronikus irat információtartalma papír alapon megjeleníthető, az elektronikus ügyintézést biztosító szerv az elektronikus iratról jogszabályban meghatározottak szerint papíralapú kiadmányt vagy másolatot készíthet vagy készíttethet.

29. § (1) A papíralapú irat hiteles elektronikus irattá alakítását a szolgáltató úgy is nyújthatja, hogy egyúttal vállalja az elektronikus ügyintézést biztosító szerv részére benyújtandó irat átvételét, majd az erről készített elektronikus másolatnak az elektronikus ügyintézést biztosító

szerv részére történő továbbítását. A szolgáltató köteles rögzíteni és a papíralapú irat átvételekor igazolni az átvétel időpontját.

(2) Az (1) bekezdés szerinti esetben a beadvány az ilyen szolgáltató részére történő átadással előterjesztettnek minősül. Az elektronikus másolat elkészítését követően a szolgáltató az eredeti papíralapú iratot

a) az elektronikus ügyintézést biztosító szerv eltérő rendelkezése hiányában visszaadja vagy visszaküldi az ügyfélnek,
b) az elektronikus ügyintézést biztosító szerv által meghatározott rendszerességgel átadja az elektronikus ügyintézést biztosító szerv részére,
c) az elektronikus ügyintézést biztosító szerv által a jogszabályi előírások figyelembevételével meghatározott esetekben és feltételekkel megsemmisíti, vagy
d) ha a szolgáltató ilyen szolgáltatást is nyújt, az elektronikus ügyintézést biztosító szerv számára megőrzi.

13. Az elektronikus dokumentumra történő rávezetés, feljegyzés, kijavítás, záradékolás, felülhitelesítés

32. § Ahol jogszabály valamely jognak, döntésnek, ténynek vagy más adatnak iratra történő feljegyzését vagy rávezetését rendeli el, valamely irat záradékolásáról vagy kijavításáról rendelkezik, az az elektronikus irat esetében történhet

a) az eredeti irathoz elektronikus formában történő csatolással úgy, hogy a csatolás egyértelmű hozzárendeléssel, elválaszthatatlan módon történik, majd az irat a csatolt adatokkal együtt felülhitelesítésre kerül, vagy
b - ha az eredeti elektronikus irat lehetővé teszi - az adatszerkezetének kiegészítésével és felülhitelesítésével, feltéve, hogy ezzel az eredeti hitelesítési információk nem sérülnek.

14. Iratkezelés, megőrzési kötelezettség teljesítése

33. § (1) Elektronikus ügyintézés esetén az egyes iratkezelési feladatok olyan szakrendszerben is megvalósíthatóak, amelynek alapfunkciója nem az iratkezelési műveletek végrehajtásának támogatása.

(2) Önmagában az (1) bekezdés szerinti szakrendszerben végzett csoportmunka - ideértve az e célra történő szignálást - nem minősül a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló törvény szerinti tanúsítás köteles tevékenységnek.

(3) Az (1) bekezdés szerinti szakrendszer úgy is megvalósítható, hogy több elektronikus ügyintézést biztosító szerv részére együttes (közös) iratkezelést valósít meg.

(4) A közfeladatot ellátó szervnek nem minősülő elektronikus ügyintézést biztosító szerv az ügyben keletkezett iratot, kép- és hangfelvételt [a (4)-(7) bekezdés alkalmazásában a

továbbiakban együtt: elektronikus irat] - ha jogszabály eltérően nem rendelkezik - e rendelet szerint köteles megőrizni. A megőrzést az elektronikus ügyintézést biztosító szerv jogszabályban meghatározott követelményeknek megfelelő szolgáltató igénybevételével is megvalósíthatja.

(5) Az elektronikus iratokat az elektronikus dokumentumtárolási szolgáltatás szabályai szerint vagy más olyan irattárolási megoldás alkalmazásával kell megőrizni, amely az elektronikus irat hitelességének tartós megőrzését is biztosítja.

(6) A (4) bekezdés szerinti elektronikus ügyintézést biztosító szerv iratkezelési szabályzatot készít, amely tartalmazza legalább:

a) az elektronikusan tárolt iratok körének meghatározását,
b) az elektronikus iratkezelés, irattárolás szabályait,
c) az elektronikusan tárolt iratok megőrzési idejét,
d) az elektronikus iratok selejtezésének rendjét.

(7) A (4) bekezdés szerinti elektronikus ügyintézést biztosító szerv esetében, ha a papíralapú iratról hiteles elektronikus másolat készült, és annak megőrzése biztosított, az eredeti papíralapú irat selejtezhető, kivéve, ha:

a) a papíralapú iratot az ügyfél számára vissza kell szolgáltatni,
b) az elektronikus másolat nem tartalmaz minden, a joghatás kiváltása és a bizonyító erő szempontjából lényeges tartalmi és formai elemet,
c) a papíralapú irat megőrzését jogszabály előírja.

54. § (1) Ha jogszabály eltérően nem rendelkezik, a törvény, illetve az elektronikus ügyintézést biztosító szerv által meghatározott határidőbe nem számít bele az a nap, amely során legalább négy órán át fennálló, üzemszünetet vagy az elektronikus ügyintézés korlátozott működőképességét okozó technikai tevékenység vagy üzemzavar akadályozta az elektronikus ügyintézést biztosító szerv elektronikus ügyintézést biztosító információs rendszerének működését.

(2) Az (1) bekezdésben foglaltak értelemszerűen alkalmazandók akkor is, ha az ügyfelet az eljárási cselekmény határidőben történő elvégzésében olyan tervezett technikai tevékenység vagy üzemzavar akadályozta, amely az általa igénybe vett szabályozott elektronikus ügyintézési szolgáltatás (a továbbiakban: SZEÜSZ) vagy központi elektronikus ügyintézési szolgáltatás (a továbbiakban: KEÜSZ) használatát érintette.

III. FEJEZET
A PAPÍRALAPÚ DOKUMENTUMOKRÓL ELEKTRONIKUS ÚTON TÖRTÉNŐ MÁSOLAT KÉSZÍTÉSÉNEK SZABÁLYAI

18. Általános szabályok

55. § (1) A papíralapú dokumentumról történő digitalizálás során a másolatkészítő biztosítja a papíralapú dokumentum és az elektronikus másolat képi vagy tartalmi megfelelését, és azt, hogy minden - az aláírás vagy bélyegző elhelyezését követően az elektronikus másolaton tett - módosítás érzékelhető legyen.

(2) Papíralapú dokumentumról történő digitalizálás során a másolat készítője elkészíti az elektronikus másolatot, megállapítja a papíralapú dokumentum és az elektronikus másolat képi vagy tartalmi megfelelését, majd ellátja az elektronikus másolatot hitelesítési záradékkal − „Az eredeti papíralapú dokumentummal egyező” − és a (4) bekezdésben meghatározott követelményeknek megfelelő elektronikus aláírással vagy bélyegzővel, és ha az időpont feltüntetése szükséges, elektronikus időbélyegzővel látja el.

(3) Ha a papíralapú dokumentum tulajdonságai miatt az elektronikus másolat nem tartalmazza a papíralapú dokumentum teljes tartalmát, a (2) bekezdésben foglaltakon túl azt is fel kell tüntetni, hogy a másolat a digitalizálás alapjául szolgáló papíralapú dokumentumot mely részében tartalmazza. Az igénylő ilyen rendelkezése esetén a másolatkészítő elektronikus kivonatot is készíthet a papíralapú dokumentumról, a másolaton rögzítve azt, hogy a készített elektronikus kivonat a papíralapú dokumentumot mely részében, a dokumentumba foglalt információtartalmat milyen korlátozásokkal tartalmazza.

(4) A másolaton minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzőt vagy olyan, minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást kell elhelyezni, amelyre vonatkozóan a bizalmi szolgáltató kizárja az álnév használatát, és igazolja, hogy a regisztráció alapjául szolgáló személyazonosság igazolására alkalmas hatósági igazolványban foglalt névvel betű szerint azonos a tanúsítványba foglalt név.

(5) Több dokumentumon is elhelyezhető egy elektronikus aláírás vagy bélyegző, illetve egy időbélyegző, valamint a (2) bekezdés szerinti megjelölések több dokumentumon együttesen is elhelyezhetőek. Ez esetben a dokumentumok a továbbiakban csak együtt kezelhetőek.

(6) A másolatkészítéssel megbízott vagy arra feljogosított személyek körét belső szabályzatban kell meghatározni.

(7) A másolatkészítőnek rendelkeznie kell a másolatkészítő rendszer olyan részletességű dokumentációjával, amelyből a rendszerrel szemben e rendeletben megállapított követelmények teljesülése megállapítható, vagy a rendszer gyártója/forgalmazója által kiállított, a megfelelésre vonatkozó igazolással.

(8) A másolatkészítőnek rendelkeznie kell a másolatkészítés eljárási és műszaki feltételeit, valamint a kapcsolódó felelősségi kérdéseket tartalmazó másolatkészítési szabályzattal. A másolatkészítő a másolatkészítési szabályzatot nyilvánosan, elektronikus úton közzéteszi.

19. Automatikus másolatkészítés

56. § (1) A másolat automatikusan is elkészíthető, ha

a) a másolatkészítés külső beavatkozástól mentes zárt rendszerben történik;
b) a másolatkészítő rendszer megfelelő műszaki és szervezési megoldással biztosítja a másolat olvashatóságát és a mintavételezésen alapuló minőségbiztosítást;
c) a záradék tartalmazza az automatikus másolatkészítés tényét.

(2) Automatikus másolatkészítés esetén a dokumentumonkénti tartalmi ellenőrzés helyett véletlenszerű mintavételezésen alapuló ellenőrzés is alkalmazható. Ha jogszabály az eredeti dokumentum megsemmisítését lehetővé teszi, az eredeti dokumentum megőrzését ilyen esetben is legalább addig biztosítani kell, amíg a másolat olvashatóságát (megnyithatóságát) a másolatkészítő vagy a másolatot felhasználó nem ellenőrizte és vissza nem igazolta.

(3) Az automatikusan készített másolatot elektronikus bélyegzővel és időbélyegzővel kell ellátni.

(4) Automatikus másolatkészítés esetében az 55. § rendelkezései alkalmazandóak.

IV. FEJEZET
A SZABÁLYOZOT T ELEKTRONIKUS ÜGYINTÉZÉSI SZOLGÁLTATÁSOK ÉS A KÖZPONTI ELEKTRONIKUS ÜGYINTÉZÉSI SZOLGÁLTATÁSOK

22. Általános követelmények

59. § (1) A SZEÜSZ, illetve KEÜSZ szolgáltató (a IV. és V. Fejezet alkalmazásában a továbbiakban együtt: szolgáltató) e szolgáltatásának nyújtása során köteles teljesíteni az e Fejezetben meghatározott követelményeket.

(2) A szolgáltató a szolgáltatás nyújtásához az alábbi követelményeknek megfelelő informatikai eszközöket, rendszereket és termékeket köteles használni:

a) az eszközök, rendszerek és termékek megbízhatóak, teljesítik a külön jogszabályban meghatározott biztonsági követelményeket, és biztosítják a jogszabályban foglalt további követelményeknek, különösen a műszaki előírásoknak és személyi feltételeknek való megfelelést,
b) a rendszerek, berendezések és termékek biztosítják, hogy a SZEÜSZ, KEÜSZ nyújtása során keletkezett adatokhoz arra jogosulatlan személyek nem férhetnek hozzá.

60. § Ha valamely kijelölt szolgáltató által nyújtott SZEÜSZ vagy KEÜSZ igénybevételét jogszabály valamely elektronikus ügyintézést biztosító szerv számára kötelezően előírja, a szolgáltatás csak olyan elérhetőség és rendelkezésre állás mellett nyújtható, amely az elektronikus ügyintézést biztosító szerv eljárási cselekményeit nem akadályozza.

61. § (1) A szolgáltató a SZEÜSZ, illetve KEÜSZ működésével kapcsolatos panaszok, kérdések fogadására telefonos ügyfélszolgálatot tart fenn, valamint erre szolgáló elektronikus űrlapon vagy elektronikus levélben vagy az ügyfél és a szolgáltató közötti kölcsönös és összefüggő adatcserét és kétirányú kapcsolatot biztosító elektronikus rendszerben a bejelentések fogadását biztosítja. A szolgáltató telefonos ügyfélszolgálata az országos telefonos ügyfélszolgálathoz csatlakozhat.

(2) Az (1) bekezdés szerinti bejelentés alapján a szolgáltató 30 napon belül köteles

a) ha az alapos, megtenni a szükséges lépéseket annak érdekében, hogy a SZEÜSZ, illetve KEÜSZ rendeltetésszerűen igénybe vehető, használható legyen, és erről a bejelentőt tájékoztatni,

b) ha az nem alapos, a bejelentés elutasításáról és annak indokairól, valamint a (3) bekezdés szerinti eljárás lehetőségéről a bejelentőt tájékoztatni.

(3) Ha a szolgáltató nem biztosítja az általános szerződési feltételek teljesülését, és az igénybevevő az (1) bekezdés szerinti bejelentése alapján a hibát határidőben nem javítja ki, vagy a bejelentést elutasítja, az igénybevevő a felügyeletnél panaszt tehet.

(4) A felügyelet a panaszt az E-ügyintézési tv. 47. § (2) és (3) bekezdésének megfelelő alkalmazásával bírálja el, és ha a panasz alapos, a szolgáltatót határozatban kötelezi a (2) bekezdés *a)* pontja szerinti eljárásra.

(5) A szolgáltató a SZEÜSZ, illetve a KEÜSZ nyújtása során tett nyilatkozatait és az egyéb ezzel összefüggő iratokat a jogszabályban foglaltak, valamint a hatósággal, illetve az ügyféllel kötött megállapodás szerint köteles megőrizni.

62. § Vélelmezni kell, hogy a SZEÜSZ-t, valamint KEÜSZ-t az arra feljogosított személy használja.

Egységes működés, együttműködési képesség

63. § (1) A szolgáltatók a SZEÜSZ-öket, KEÜSZ-öket úgy alakítják ki és úgy szolgáltatják, hogy azok alkalmasak legyenek az elektronikus ügyintézést biztosító és az együttműködő szervek informatikai rendszerei közötti együttműködésre.

(2) A felügyelet az (1) bekezdés szerinti együttműködés előmozdítása érdekében ajánlásokat bocsát ki, valamint együttműködik a szolgáltatóval a SZEÜSZ, illetve KEÜSZ e követelménynek megfelelő kialakítása érdekében.

Általános szerződési feltételek

64. § (1) SZEÜSZ, illetve KEÜSZ a felügyelethez benyújtott általános szerződési feltételek alapján nyújtható. A szolgáltató és a szolgáltatás igénybe vevője közös megegyezéssel eltérhetnek a felügyelethez benyújtott általános szerződési feltételekben foglaltaktól.

(2) Ha a szolgáltató több SZEÜSZ-t, illetve KEÜSZ-t együttesen nyújt, a szolgáltatások tekintetében jogosult egységes, összevont általános szerződési feltételek, illetve szolgáltatási szabályzat készítésére.

(3) Az általános szerződési feltételek tartalmazzák legalább az alábbiakat:

a) a szolgáltatási időszakot, rendelkezésre állást,
b) a szolgáltatások elérhetőségét, jogosultsági kérdéseket,
c) a felhasználói támogatás feltételeit,
d) a funkcionalitást,
e) az igénybevétel technikai feltételeit, ideértve a műszaki és adminisztratív feltételeket,
f) az igénybevétel pénzügyi feltételeit,
g) a bejelentések, panaszok kezelésének rendjét,
h) a szolgáltató felelősségére vonatkozó rendelkezéseket.

(4) A felügyelethez benyújtott általános szerződési feltételeket a szolgáltató az elektronikus tájékoztatás szabályai szerint közzéteszi.

(5) Ha a KEÜSZ, SZEÜSZ bizalmi szolgáltatásnak minősül, a (3) bekezdésben előírt információkat az általános szerződési feltételek helyett a szolgáltatási szabályzat is tartalmazhatja.

A szolgáltatásnyújtásra vonatkozó szervezési feltételek

65. § (1) A szolgáltató a SZEÜSZ, KEÜSZ nyújtásához köteles kijelölni és a felügyelet felé bejelenteni az alábbiakat:

a) a szolgáltatásért felelős vezető személyét,
b) a szolgáltatás ellenőrét,
c) a szolgáltatás biztonsági felelősét.

(2) Ha a SZEÜSZ, KEÜSZ jellege megköveteli, a szolgáltató műszaki, technikai jellegű kérdésekben illetékes kapcsolattartót is kijelöl, akinek elérhetőségét az elektronikus tájékoztatás szabályai szerint közzéteszi.

66. § A SZEÜSZ-t, KEÜSZ-t - az adott SZEÜSZ-re, KEÜSZ-re vonatkozó eltérő rendelkezés hiányában - legalább félévente a biztonsági felelős útján, évente pedig az az ellenőr útján az általános szerződési feltételeknek vagy szolgáltatási szabályzatnak megfelelés szempontjából ellenőrizni kell. Az ellenőrzés tényét és eredményét jegyzőkönyvben kell rögzíteni.

A szolgáltatásnyújtásra vonatkozó biztonsági követelmények

67. § (1) A SZEÜSZ, KEÜSZ nyújtásához alkalmazott informatikai rendszernek biztosítania kell, hogy:

a) a rendszerben található adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása az adatkezelést szabályozó törvényi előírások betartásával történjen (törvényes adatkezelés),

b) a rendszerben kezelt, tárolt adatot csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhessék meg, használhassák fel, illetve rendelkezhessenek annak felhasználásáról (bizalmasság),

c) a rendszerben kezelt adat tartalma és tulajdonságai az elvárttal megegyezzenek - ideértve a bizonyosságot abban, hogy az elvárt forrásból származik, és a származás ellenőrizhetőségét, bizonyosságát is -, továbbá a rendszerelemek a rendeltetésüknek megfelelően használhatóak legyenek (sértetlenség),

d) a rendszerben kezelt adatokat, illetve az informatikai rendszer elemeit az arra jogosultak a szükséges időpontban és időtartamra használhassák (rendelkezésre állás),

e) érvényesüljenek a zárt, teljes körű, folytonos és a kockázatokkal arányos védelem követelményei.

(2) Az (1) bekezdésben meghatározott követelmények teljesülése érdekében a szolgáltatónak meg kell felelnie az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény és végrehajtására kiadott rendeletekben foglalt feltételeknek, és a szolgáltatást - valamint, ha elkülönült egységet alkotnak, a részszolgáltatást - nyújtó informatikai rendszert is e jogszabályok szerinti biztonsági osztályba kell sorolni.

23. Kötelezően igénybe veendő központi elektronikus ügyintézési szolgáltatások

68. § Az elektronikus ügyintézést biztosító szerv köteles biztosítani az e-Papír szolgáltatás útján előterjesztett beadványok befogadását, ha az adott ügytípus elektronikus űrlappal nem támogatott.

23/A. Szabályozott, illetve központi elektronikus ügyintézési szolgáltatások elektronikus ügyintézést nem biztosító szerv általi igénybevétele

68/A. § (1) Az elektronikus ügyintézést biztosítónak nem minősülő gazdálkodó szervezet (a továbbiakban: piaci szereplő) a SZEÜSZ-t, valamint KEÜSZ-t - a (2) bekezdésben meghatározott kivétellel - a 2. melléklet szerint megállapított díj megfizetése ellenében veheti igénybe. A piaci szereplő és az adott SZEÜSZ, illetve KEÜSZ nyújtására a SZEÜSZ vagy KEÜSZ szolgáltató szerződést köt. A piaci szereplőt az igénybevétel során az adott SZEÜSZ és KEÜSZ felhasználása tekintetében elektronikus ügyintézést biztosító szervnek kell tekinteni.

(2) Az EFER tranzakciós díjak és a Magyar Államkincstár által alkalmazott, átutalási műveletekhez kapcsolódó díjak, valamint az dokumentumtárolási szolgáltatáshoz kapcsolódó tárhelyszolgáltatás kapacitásdíja kivételével nem köteles díj fizetésére a piaci szereplő, ha

a) állami vagy önkormányzati költségvetési szerv, vagy
b) ha jogszabályban meghatározott, kizárólag központi költségvetési forrásból fedezett vagy központi költségvetési forrásból 100%-ig támogatott állami közfeladatának elősegítése érdekében veszi igénybe a SZEÜSZ-t, valamint a KEÜSZ-t.

(3) Piaci szereplő nem vehet igénybe a kormányzati hitelesítésszolgáltató által nyújtott bizalmi szolgáltatást.

(4) Nincs helye az (1) bekezdés szerinti, az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló Korm. rendeletben SZEÜSZ vagy KEÜSZ nyújtására kijelölt szolgáltató (a továbbiakban: a Kormány rendeletében kijelölt szolgáltató) esetében a szerződés megkötésének, ha a tervezett igénybevétel

a) veszélyezteti más igénybevevők vagy az érintett szolgáltatók információbiztonságát,
b) veszélyezteti az elektronikus ügyintézést biztosító szervek részére nyújtott szolgáltatások megfelelő színvonalú biztosítását,
c) biztosítása aránytalan nehézséggel vagy költséggel járna,
d) során a SZEÜSZ-t vagy KEÜSZ-t igénybevevő információs rendszer vagy szolgáltatás közrendbe vagy jóerkölcsbe ütközik,
e) során a piaci szereplő az előírt technikai feltételeknek nem felel meg, vagy
f) során az érintett információs rendszer jogszabályban foglalt egyéb feltételnek nem felel meg.

(5) A Kormány rendeletében kijelölt szolgáltató a SZEÜSZ vagy KEÜSZ igénybevételére vonatkozó szerződést felmondhatja

a) a (4) bekezdés szerinti okból, vagy
b) ha az igénybevevő nem teljesíti a szerződésben vállalt kötelezettségeit.

68/B. § (1) A KEÜSZ vagy SZEÜSZ szolgáltató az igénybevételt megelőzően legalább 30 nappal köteles előzetesen tájékoztatni a felügyeletet a SZEÜSZ, illetve KEÜSZ piaci szereplő általi igénybevételéről.

(2) A Kormány rendeletében kijelölt szolgáltató esetében a 68/A. § (1) bekezdés szerinti szerződés megkötéséhez, valamint a szerződés felmondásához

a) ha az állam minősített többséggel rendelkezik a szolgáltató felett, a tulajdonosi jogokat gyakorló,
b) a költségvetési szerv tekintetében a felügyeletet gyakorló

miniszter jóváhagyása szükséges. A miniszter a döntését nem köteles indokolni.

(3) A SZEÜSZ, valamint a KEÜSZ piaci szereplő általi igénybevétele esetében a felügyelet az E-ügyintézési tv. 46-48. §-ában és e rendeletben foglalt rendelkezések szerint jár el.

Biztonságos kézbesítési szolgáltatás

73. § (1) A biztonságos kézbesítési szolgáltatás olyan kézbesítési szolgáltatás, amely az elektronikus üzenet kézbesítésével kapcsolatban biztosítja az alábbi feltételek mindegyikének teljesülését:

a) az üzenet fogadásának igazolása: ha a küldőtől átvett üzenetet a kézbesítési rendszer átvette, akkor erről a feladó számára feladást igazoló elektronikus okirat (e § alkalmazásában a továbbiakban: okirat) áll rendelkezésre;
b) sértetlenség: az üzenet és a kézbesítést igazoló okirat észrevétlenül nem változtatható meg sem a kézbesítés során, sem a kézbesítést követően;
c) az átvevő igazolása: az üzenet átvevője csak a címzett vagy a feljogosított helyettes átvevő lehet, és a feladó számára a tényleges átvevőt az átvétellel kapcsolatos okirat igazolja;
d) sikertelen kézbesítés igazolása: a feladónak okirat áll rendelkezésére arról az esetről is, ha a kézbesítés a megadott határidőn belül sikertelen; az igazolás a meghiúsulás időpontját és - ha azonosítható - okát tartalmazza.

(2) A biztonságos kézbesítési szolgáltatásnak továbbá biztosítania kell, hogy a címzett számára az üzenet elkülönített, a szolgáltató felügyelete alatt álló informatikai rendszerben legalább az (1) bekezdés *d)* pontja szerinti okirat kiállításáig hozzáférhető.

(3) A biztonságos kézbesítési szolgáltatás alapjául szolgáló informatikai rendszernek biztosítania kell a rendszer zártságát, a jogosulatlan változtatások kizárását. A szolgáltató köteles e követelményeknek való megfelelést a felügyelet részére tanúsítvánnyal igazolni, majd a szolgáltatás nyújtása során a tanúsítványt annak lejárta előtt folyamatosan megújítani, az új tanúsítványt a felügyeletnek benyújtani.

74. § A biztonságos kézbesítési szolgáltató köteles általános szerződési feltételeiben szabályozni az üzenet feladásának és fogadásának feltételeit, így különösen, hogy

a) a feladó mely címzettnek küldhet üzenetet,
b) a feladó milyen formátumú üzeneteket küldhet (különösen mellékletek csatolhatósága, méret- és formátummegkötések),
c) a feladó az üzenetet hol és milyen módon adhatja fel,
d) a szolgáltató az üzenetet mikor és milyen módon bocsátja a címzett rendelkezésére,
e) a címzett miként rendelkezhet a nevében az üzenet fogadására jogosult helyettes átvevőről,
f) a címzett miként rendelkezhet arról, hogy a meghatározott időtartam alatt vagy a jövőben részére érkező üzeneteket másik biztonságos kézbesítési szolgáltatáshoz tartozó címre továbbítsák, az üzenet fogadását visszautasítsák,
g) a szolgáltatás során a címzettet vagy a feladót a másik fél, illetve a szolgáltató milyen módon azonosíthatja,

h) az üzenet feladása és fogadása milyen esetben és milyen módon igényli a szolgáltató közreműködését,

i) az üzenet feladását, illetve az átvételt igazoló igazolást ki állítja ki, és ahhoz milyen módon jut hozzá a feladó, illetve a címzett,

j) melyek a kézbesítéssel, illetve a kézbesítéssel kapcsolatos egyes tevékenységek elvégzésével kapcsolatos időbeli korlátok, és ezek túllépésének mi a következménye,

k) a szolgáltató az általa továbbított üzenet tartalmát megismerheti-e, helyre tudja-e állítani, és ha igen, milyen esetben,

l) mi az át nem vett üzenet sorsa, megsemmisítésének vagy visszaküldésének módja és ütemezése,

m) milyen informatikai és nem informatikai eszközökkel biztosítja a szolgáltató a levéltitok megőrzését, valamint

n) a szolgáltatón, a feladón és a címzetten kívül ki és milyen esetben ismerheti meg az üzenet tartalmát.

75. § (1) A 73. § (1) bekezdése szerinti kézbesítéssel kapcsolatos események tekintetében a szolgáltató haladéktalanul olyan igazolást köteles kiállítani a feladónak az általa megadott elektronikus elérhetőségére, amely a kézbesítési események adatait megfelelően igazolja. A szolgáltató a kézbesítési események adatait - kiállított igazolásonként vagy együttesen - tárolja.

(2) A szolgáltató az igazolásokat alapvetően elektronikus formában biztosítja, de - ha a vonatkozó KEÜSZ nyújtására jogosult - a kézbesítést kérő vagy címzett kérésére a rájuk vonatkozó igazolásról hiteles papíralapú másolatot készít.

(3) Az (1) bekezdés szerinti igazolás a szolgáltató részéről legalább fokozott biztonságú elektronikus bélyegzővel hitelesített és időbélyegzővel ellátott, valamint tartalmazza a feladó megnevezését, az üzenet lenyomatát és az érkeztetőszámot.

76. § A biztonságos kézbesítési szolgáltatás igénybevételével kézbesített iratnál az átvételre jogszabály eltérő rendelkezése hiányában 5 munkanapot kell biztosítani. Ha a címzett a küldeményt a határidőn belül nem veszi át, és az átvételt nem tagadja meg, akkor a kézbesítésről - az első kézbesítési kísérletre vonatkozó szabályok megfelelő alkalmazásával - az 5. munkanap elteltét követő első munkanapon másodszor is értesítést kap.

77. § Jogszabály egyes beadványok benyújtását biztonságos kézbesítési szolgáltatásnak nem minősülő elektronikus kézbesítési szolgáltatás alkalmazása esetén is lehetővé teheti, ha az az E-ügyintézési tv. szerinti hivatalos elérhetőség feltételeinek megfelel.

Kormányzati elektronikusaláírás-ellenőrzési szolgáltatás

81. § (1) A szolgáltatás keretében a szolgáltató biztosítja az elektronikus dokumentumon elhelyezett elektronikus aláírás, elektronikus bélyegző érvényességének ellenőrzését.

(2) A szolgáltató köteles biztosítani az elektronikus aláírás, elektronikus bélyegző ellenőrzését az elektronikus dokumentum alapján, függetlenül attól, hogy az elektronikus aláírás, elektronikus bélyegző a dokumentumhoz kapcsolt, vagy külön adatszerkezetként kezelendő.

(3) Az ellenőrzés részeként a szolgáltató

a) ellenőrzi az elektronikus aláírás, elektronikus bélyegző érvényességét, valamint
b) a dokumentum ellenőrizhetősége esetén ellenőrzi a dokumentum sértetlenségét,
c) az ellenőrzés eredményéről igazolást állít ki.

(4) A tanúsítvány érvényességét a szolgáltató

a) ha az rendelkezésre áll és ingyenes, azonnali tanúsítványállapot-igazoló szolgáltatással, vagy
b) ha az azonnali tanúsítványállapot-igazoló szolgáltatás nem érhető el, a visszavonási állapotinformációk segítségével

ellenőrzi.

(5) A szolgáltató biztosítja az illetékes hatóságok által a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti és tanácsi irányelv alapján elektronikusan aláírt dokumentumok országhatáron átnyúló feldolgozására vonatkozó minimumkövetelményekről szóló 2011/130/EU határozat módosításáról szóló 2014/148/EU bizottsági végrehajtási határozatban meghatározott szabványformátumok feldolgozására vonatkozó rendelkezéseknek történő megfelelést.

Kézbesítési szolgáltatás

82. § (1) A kézbesítési szolgáltatás keretében a SZEÜSZ szolgáltató közreműködik valamely elektronikus nyilatkozat (jelen alcím alkalmazásában a továbbiakban: üzenet) kézbesítésével összefüggő egy vagy több alábbi tevékenységben, illetve ezen tevékenységek bizonyításában:

a) az üzenet átvétele a feladótól,
b) az üzenet továbbítása a címzettnek vagy a kézbesítésben közreműködő köztes harmadik személynek,
c) az üzenetnek a címzett rendelkezésére bocsátása olyan módon, hogy a címzett a kézbesített üzenet tartalmát értelmezhető módon megismerhesse, és így az üzenetről tudomást szerezhessen (jelen alcím alkalmazásában a továbbiakban: az üzenet fogadása),
d) az üzenet tárolása a címzett számára legfeljebb az általános szerződési feltételekben meghatározott időpontig,
e) az üzenet titkosítása vagy egyéb módon történő olvashatatlanná tétele az üzenet fogadásáig, valamint az üzenet fogadása végett az üzenet titkosításának feloldása vagy az üzenet olvashatóvá tétele,
f) a feladó vagy a címzett értesítése a kézbesítéssel kapcsolatos egyes tényekről,
g) a feladó vagy a címzett kézbesítési szolgáltatással kapcsolatos egyes nyilatkozatainak tárolása.

(2) Kézbesítési szolgáltatásnak minősül a felügyelet által kiadott ajánlásban megadott műszaki követelményeket kielégítő, internetes felületen biztosított dokumentum le-, illetve feltöltés biztosítása is, ha

a) feltöltés esetén a címzett elektronikus ügyintézést biztosító szerv a felületen egyértelműen azonosított, illetve
b) letöltés esetén a letöltést csak azonosítás mellett, kizárólag a címzettnek teszik lehetővé.

(3) Az (1) bekezdésben felsorolt tevékenységeket az elektronikus ügyintézést biztosító szerv vagy SZEÜSZ szolgáltató is végezheti. Az egyes tevékenységek több SZEÜSZ szolgáltató között is megoszthatóak.

(4) A SZEÜSZ szolgáltató a kézbesítési szolgáltatáshoz külön szolgáltatásokat biztosíthat, így különösen

a) címlistára történő továbbítást,
b) üzenet illetéktelen megismerés elleni fokozott védelmét biztosító szolgáltatást, valamint
c) időponthoz kötött kézbesítést.

83. § (1) A kézbesítési szolgáltatás igénybevételének feltétele, hogy a feladó megadja a címzettnek a SZEÜSZ szolgáltató által értelmezhető és kezelhető kézbesítési címét.

(2) Kézbesítési címként az elektronikus ügyintézést biztosító szervek által küldött értesítéseknél az ügyfél ügyintézési rendelkezésében megadott hivatalos vagy annak megfelelő elérhetőség vehető figyelembe. Ha az ügyfél ilyet nem adott meg, vagy a megadott cím hibás, a kézbesítés céljára felhasználható

a) az eljárás során az ügyfél által megadott elektronikus elérhetőség vagy
b) az elektronikus ügyintézést biztosító szerv vagy a SZEÜSZ szolgáltató által egyébként nyilvántartott elektronikus elérhetőség.

(3) A címzett által megadott kézbesítési cím létezéséről, működőképességéről a SZEÜSZ szolgáltató a feladást megelőzően nem köteles meggyőződni.

(4) Arról az üzenetről, amelyet a SZEÜSZ szolgáltatón kívül álló okból a címzettnek vagy az átvételre jogosult más személynek nem lehet kézbesíteni, a feladó részére igazolást szükséges kiállítani, és számára elérhetővé tenni.

(5) Ha a kézbesíthetetlen üzenet a feladó részére nem küldhető vissza, a SZEÜSZ szolgáltató az üzenetet törli.

25. Az egyes központi elektronikus ügyintézési szolgáltatásokra vonatkozó rendelkezések

Az ügyfél ügyintézési rendelkezésének nyilvántartása

92. § (1) A rendelkezési nyilvántartás KEÜSZ szolgáltatója legalább az alábbi tárgykörökben biztosítja az ügyfél számára jognyilatkozat, rendelkezés tételének lehetőségét:

a) elektronikus kapcsolattartás megengedhetőségére vonatkozó rendelkezés,
b) ügyfél által lehetővé tett elektronikus vagy nem elektronikus kapcsolattartási formák,
c) azonosítással kapcsolatos követelmények,
d) hivatalos elektronikus kapcsolattartásra szolgáló elérhetőségek,
e) elektronikus dokumentumok titkosítására vonatkozó igény,
f) elektronikus ügyintézési cselekményekről időszaki értesítés igénylése,
g) képviseletre vonatkozó jognyilatkozatok.

(2) Az ügyintézési rendelkezésben tehető jognyilatkozatok körét - ideértve az (1) bekezdésben nem szereplő lehetséges jognyilatkozatok körét - a szolgáltató az elektronikus tájékoztatás szabályai szerint közzéteszi.

(3) A rendelkezési nyilvántartás szolgáltatója biztosítja, hogy az ügyfél az ügyintézési rendelkezések nyilvántartásában rögzítse a 24. §-ban meghatározott követelményeknek megfelelő titkosítási célú nyilvános kulcsot.

93. § (1) Az ügyintézési rendelkezés első alkalommal kizárólag személyes megjelenés mellett tehető. Az első alkalommal történő ügyintézési rendelkezéstétel során az ügyintézési rendelkezés tételét biztosító szerv

a) természetes személy esetében
aa) a nyilatkozattevő személyazonosságát személyazonosító okmánnyal ellenőrzi, valamint
ab) közhiteles nyilvántartásban ellenőrzi a nyilatkozattevő által használt okmányokat és adatokat,
b) szervezet esetében
ba) a szervezetnek megfelelő közhiteles nyilvántartásban ellenőrzi a szervezet adatait,
bb) a szervezet nevében nyilatkozó személyt az *a)* pont szerint azonosítja, és ellenőrzi a képviseleti jogosultságát, valamint
bc) a nyilatkozattételt követően a szervezetet haladéktalanul értesíti a szervezet képviseletében tett ügyintézési rendelkezésről.

(2) Az (1) bekezdéstől eltérően az első rendelkezés az ügyintézési rendelkezések nyilvántartásának felületén, elektronikus úton is megtehető

a) az eIDAS Rendelet 6. cikk (1) bekezdése szerinti feltételeknek megfelelő elektronikus azonosítóeszközzel vagy
b) természetes személy ügyfél esetében, ha rendelkezik KASZ-szal, és azzal azonosítja magát,
c) gazdálkodó szervezet és egyéb nem természetes személy esetében, ha az önálló képviseletre jogosult képviselője vagy meghatalmazottja rendelkezik KASZ-szal, és azzal azonosítja magát, és képviseleti jogosultságát is igazolja.

(3) Az ügyintézési rendelkezést a nyilatkozatot tevő személy - a telefonos ügyfélszolgálatnál tett nyilatkozat kivételével - aláírásával vagy az elektronikus dokumentumhitelesítésre vonatkozó rendelkezések szerint hitelesíti. A telefonos ügyfélszolgálatnál tett nyilatkozatot az ügyfél azonosítását követően az ügyfélszolgálat írásban rögzíti, a személyhez rendelést záradékban igazolja, és azt az elektronikus dokumentumhitelesítés szabályai szerint hitelesíti.

(4) A szolgáltató az ügyintézési rendelkezések nyilvántartása alapján kiállított, általa hitelesített igazolásban automatikus információátadás útján, a 134. § szerinti ügynöki szolgáltatás igénybevételével vagy más, automatizált feldolgozásra alkalmas módon tájékoztatja az elektronikus ügyintézést biztosító szervet vagy más szolgáltatót az ügyintézési rendelkezés tartalmáról.

94. § (1) Az ügyfél az ügyintézési rendelkezésben adott meghatalmazás tekintetében a meghatalmazás terjedelmét meghatározhatja

a) a szolgáltató által közzétett lista használatával vagy
b) szabadszöveges meghatározással.

(2) Az ügyintézési rendelkezésben adott meghatalmazás automatizált ügyintézés céljára kizárólag az (1) bekezdés *a)* pontja szerinti meghatalmazás esetében használható fel.

(3) Az ügyintézési rendelkezésben meghatalmazás telefonon is adható, valamint elfogadható. A szolgáltató a meghatalmazással kapcsolatos jognyilatkozatokat telefonos ügyfélszolgálatán, a Kormány által kötelezően nyújtott, telefonos személyazonosításra alkalmas azonosítási szolgáltatások közül a szolgáltató által lehetővé tett azonosítási technikák közül, az ügyfél ügyintézési rendelkezésében engedélyezett azonosítás megkövetelése mellett fogadja.

(4) Az ügyintézési rendelkezések nyilvántartását vezető szerv ügynöki szolgáltatás útján az e-ügyintézést biztosító szerv kérelme alapján ellenőrizheti, és - sikeres ellenőrzés esetén - igazolhatja a képviseleti jogosultságot az egyes képviseleti jogosultságokat tartalmazó nyilvántartásokból.

(5) A meghatalmazott az ügyben a képviseleti jogosultságát az ügyintézési rendelkezések nyilvántartására hivatkozással is igazolhatja. A meghatalmazást az elektronikus ügyintézést biztosító szerv vagy más szolgáltató a meghatalmazás azonosítójának vagy a meghatalmazott azonosító adatainak megadásával kérdezheti le.

95. § Nem elektronikus ügyintézés esetén az elektronikus űrlapon adott meghatalmazásról az elektronikus ügyintézést biztosító szerv - az ügyfél vagy meghatalmazottja kérelmére - az eljáró szerv számára a meghatalmazás érvényességének e rendeletben előírt, a rendelkezési nyilvántartásban történő lekérdezése céljából képi formátumú elektronikus, valamint papíralapú hiteles vagy nem hiteles másolat készítését biztosítja. A papíralapú másolaton a meghatalmazás nyilvántartási azonosítóját is fel kell tüntetni.

96. § A szolgáltató a halál, illetve a jogutód nélküli megszűnés időpontjától számított 10 év elteltével törli a személyre vonatkozó adatokat.

Iratérvényességi nyilvántartás

97. § (1) Az iratérvényességi nyilvántartás KEÜSZ szolgáltatás (ezen alcím alkalmazásában a továbbiakban: nyilvántartás) az elektronikus ügyintézést biztosító szerv által készített elektronikus dokumentumok, illetve az elektronikus dokumentumokról készített papíralapú

hiteles másolatok tartalmának és hitelességének ellenőrzését biztosító nyilvántartás, amely a nyilvántartásban elhelyezett iratok hitelességét jelen alcím szerinti megoldásokkal biztosítja.

(2) A nyilvántartásba bejegyzést csak

a) az adott iratot kiadmányozó elektronikus ügyintézést biztosító szerv,
b) az iratról hiteles másolatot készítő szervezet, valamint
c) az irat hitelességéről igazolás kiállítására jogosult szerv vagy szervezet tehet.

(3) A szolgáltató a nyilvántartásra vonatkozó általános szerződési feltételekben rögzíti, hogy a nyilvántartás tartalmához történő hozzáférés milyen feltételekkel lehetséges.

(4) Az iratérvényességi nyilvántartás igénybevétele legfeljebb az E-ügyintézési tv. 18. § (6) bekezdése szerinti azonosításhoz köthető.

(5) A szolgáltató köteles gondoskodni az illetéktelen hozzáférés megakadályozásáról.

98. § (1) Elektronikus irat hiteles papíralapú irattá alakítása kijelölt szolgáltató általi nyújtása során a nyilvántartás az eredeti elektronikus irat elérhetőségi adatait, az irat lenyomatát, valamint az irat szöveges tartalmának lenyomatát tartalmazza. Ebben az esetben az eredeti elektronikus irat megőrzéséről és elérhetőségéről az elektronikus irat hiteles papíralapú irattá alakítása KEÜSZ-t igénybe vevő csatlakozott szervezet gondoskodik. Az elektronikus irat hiteles papíralapú irattá alakítása kijelölt szolgáltatója a hiteles másolaton köteles elhelyezni az irat lenyomatát, az irat szöveges tartalmának lenyomatát, valamint az eredeti elektronikus irat, illetve az iratérvényességi nyilvántartásban tárolásra kerülő lenyomatok elérhetőségi adatait. A lenyomatokat és a dokumentum elérhetőségét az iratérvényességi nyilvántartásban is el kell helyeznie.

(2) Az (1) bekezdés szerinti esetben a papíralapú másolat hitelesnek tekintendő, ha az ellenőrzési folyamat során a papíralapú irat egyezése megállapítható az eredeti elektronikus dokumentummal, és az eredeti irat lenyomatának és az iratérvényességi nyilvántartásban rögzített lenyomatnak az egyezése is megállapítható. Ha az ellenőrzés során az egyezés nem állapítható meg, az elektronikus ügyintézést biztosító szerv által tárolt elektronikus dokumentum, valamint a papíralapú másolat hitelessége az elektronikus ügyintézést biztosító szerv által tárolt elektronikus dokumentum tartalma, a papíralapú másolat tartalma, valamint az ezek alapján képzett, illetve a nyilvántartásban tárolt lenyomatok összevetése alapján állapítandó meg.

Azonosításra visszavezetett dokumentumhitelesítés

112. § (1) Az azonosításra visszavezetett dokumentumhitelesítés (a továbbiakban: AVDH) KEÜSZ keretében a szolgáltató a személyhez rendelésről kiállított igazolást elektronikus dokumentumba vagy az elektronikus dokumentumhoz kapcsolt záradékba foglalja, és azt - a hitelesítendő nyilatkozattal együtt - minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzővel, valamint minősített időbélyegzővel hitelesíti.

(2) Az (1) bekezdés szerinti igazolás tartalmazza

a) az ügyfél nevét és a rendelkezésére álló azonosító adatok közül az ügyfél által megjelölt és

az AVDH szolgáltatója által az azonosítási szolgáltatónál, a központi azonosítási ügynök, a rendelkezési nyilvántartás vagy az összerendelési nyilvántartás igénybevételével lekérdezett adatokat, valamint

b) a nyilatkozat további azonosító adatait.

(3) Ha a nyilatkozatot több személyhez kell rendelni, a szolgáltató az egyes személyekhez rendelés során az (1) és (2) bekezdés megfelelő alkalmazásával jár el.

(4) Az e § rendelkezései szerint kiállított okirat teljes bizonyító erejű magánokirat.

113. § (1) Az AVDH KEÜSZ elektronikus ügyintézést biztosító szerv számára a nevében eljáró személy nyilatkozatának hitelesítésére az e §-ban meghatározott eltérésekkel nyújtható.

(2) A szolgáltató részére a nyilatkozattevő személyére vonatkozó azonosító adatokat a hitelesítést kérő hivatali programrendszer adja át a hivatali programrendszerben alkalmazott felhasználó azonosítási rendszer adatai alapján.

(3) A szolgáltató által kiállított igazolás tartalmazza

a) a nyilatkozattevő nevét, beosztását, szervezeti egységét, a szervezet megnevezését és a nyilatkozattevő szervezeten belüli egyedi azonosítóját,

b) a nyilatkozat további azonosító adatait.

(4) Az e § szerint hitelesített okirat közokirat, ha azt bíróság, közjegyző, ügyész vagy más hatóság, illetve közigazgatási szerv ügykörén belül, a jogszabályi rendelkezéseknek megfelelő módon állította ki.

Központi érkeztetési ügynök

117. § (1) A központi érkeztetési ügynök (a továbbiakban: KÉÜ) KEÜSZ szolgáltatója biztosítja az elektronikus ügyintézést biztosító szerv által egyenként is igénybe vehető alábbi részszolgáltatásokat:

a) közfeladatot ellátó szervnek minősülő elektronikus ügyintézést biztosító szerv számára a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló kormányrendeletben az elektronikus úton érkezett küldemények átvétele, felbontása és érkeztetése tekintetében meghatározott egyes feladatok ellátása;

b) az elektronikus dokumentumnak az elektronikus ügyintézést biztosító szerv által kijelölt kapcsolattartási módon történő átvétele;

c) ha ez lehetséges, a feladó ügyintézési rendelkezésének való megfelelés ellenőrzése;

d) a dokumentum biztonsági ellenőrzése;

e) a dokumentum formátumának ellenőrzése;

f) elektronikus aláírással vagy bélyegzővel ellátott küldemény esetén az elektronikus aláírás vagy bélyegző érvényességének ellenőrzése, valamint jogszabály rendelkezése vagy a közfeladatot ellátó szervvel kötött megállapodás alapján a hosszú távú letagadhatatlansághoz szükséges kellékek biztosítása;

g) a dokumentum elektronikus ügyintézést biztosító szerv nevében történő átvételének hivatalos visszaigazolása vagy - az igénybevevő által meghatározott esetekben - az átvétel hivatalos megtagadása;

h) a dokumentum, valamint az érkeztetési nyilvántartás adatainak a címzett elektronikus ügyintézést biztosító szerv részére történő átadása.

(2) A KÉÜ szolgáltatója a küldemény átvétele, felbontása és érkeztetése során az elektronikus ügyintézést biztosító szerv adatfeldolgozójaként jár el.

(3) A KÉÜ a küldemény átvételét, felbontását és érkeztetését követően az elektronikus ügyintézést biztosító szerv részére az érkeztetési nyilvántartás adataival együtt, ha ez lehetséges, olyan formában adja át, hogy azt a címzett elektronikus ügyintézést biztosító szerv iratkezelő rendszere automatikusan érkeztetni tudja. A KÉÜ az elektronikus ügyintézést biztosító szerv rendelkezése alapján az érkeztetési nyilvántartás adatait közvetlenül az elektronikus ügyintézést biztosító szerv iratkezelő rendszere számára adja át, az elektronikus ügyintézést biztosító szerv iratkezelő rendszere - ha az iratkezelési szabályzata ezt lehetővé teszi - az érkeztetési nyilvántartás adatait automatikusan is bevezetheti iratkezelő rendszerébe.

Központi kézbesítési ügynök

118. § (1) A központi kézbesítési ügynök (a továbbiakban: KKÜ) KEÜSZ szolgáltatója biztosítja az elektronikus ügyintézést biztosító szerv által részlegesen is igénybe vehető alábbi részszolgáltatásokat:

a) közfeladatot ellátó szervnek minősülő elektronikus ügyintézést biztosító szerv számára a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló kormányrendeletben meghatározott egyes elektronikus úton történő küldemény küldésével kapcsolatos feladatok ellátása, valamint az adathordozó fajtájának meghatározása;

b) a küldeménynek az elektronikus ügyintézést biztosító szervtől történő átvétele;

c) a küldemény kiküldés előtti biztonsági ellenőrzése;

d) a jogszabályoknak és - ha a címzett személye automatikusan megállapítható, valamint a rendelkezési nyilvántartással a kapcsolat biztosított - a címzett ügyintézési rendelkezésének megfelelő kézbesítési forma, mód és cím megválasztása;

e) a küldemény elektronikus bélyegzővel való hitelesítése;

f) a küldemény *d)* pont szerinti kézbesítési mód és forma szerinti, kézbesítési címre történő kézbesítése iránti intézkedés;

g) a küldemény elküldését, valamint kézhezvételét igazoló visszaigazolás átvétele és az elektronikus ügyintézést biztosító szervnek történő átadása, ha a kézbesítési szolgáltatás részeként ilyen kiállításra kerül;

h) a kézbesítés iránt történő intézkedés időpontjának és módjának az elektronikus ügyintézést biztosító szervvel való haladéktalan közlése.

(2) Az elektronikus ügyintézést biztosító szerv a küldeményt az (1) bekezdés szerinti feladatok ellátásához szükséges adatokkal együtt adja át a KKÜ szolgáltató részére.

(3) A KKÜ szolgáltató a kézbesítésre átadott küldemények kézbesítési rendszerben használt azonosítójáról nyilvántartást vezet.

(4) Ha az elektronikus ügyintézést biztosító szerv a KÉÜ szolgáltatást a KKÜ szolgáltatással közösen veszi igénybe,

a) a KKÜ szolgáltató a kézbesítésre átadott küldemények kézbesítési rendszerben használt azonosítójáról vezetett nyilvántartást a KÉÜ szolgáltató számára hozzáférhetővé teszi annak érdekében, hogy a KÉÜ szolgáltató a kézbesítés eredményéről érkező visszajelzéseket a kézbesítésre átadás adataihoz csatoltan tudja az elektronikus ügyintézést biztosító szerv számára megadni,

b) a KÉÜ szolgáltató a kézbesítések eredményéről érkező igazolásokat a KKÜ szolgáltató által hozzáférhetővé tett nyilvántartás alapján a küldésre vonatkozó adatokhoz csatoltan adja át az elektronikus ügyintézést biztosító szervnek.

(5) A KKÜ szolgáltatója a szolgáltatás nyújtása során az igénybevevő adatfeldolgozójaként jár el.

Papíralapú irat átalakítása hiteles elektronikus irattá

121. § (1) A papíralapú irat hiteles elektronikus irattá alakítása során

a) az elektronikus ügyintézést biztosító szerv saját feladatkörében,

b) a központi érkeztető rendszer az E-ügyintézési tv. 74. § (3) bekezdés *a)* pontjában meghatározott feladatkörében, valamint

c) a papíralapú irat hiteles elektronikus irattá alakítása KEÜSZ kijelölt szolgáltatója a III. Fejezetben foglaltak szerint jár el az e §-ban foglalt eltérésekkel.

(2) Az elektronikus másolatot a következő metaadatok elhelyezésével kell létrehozni, és azt egyértelműen az eredeti papíralapú dokumentumhoz rendelni:

c) a másolatkészítő szervezet elnevezése és - ha a másolatkészítés nem az automatikus másolatkészítés 55. §-ban meghatározott szabályai szerint történik - a másolat képi vagy tartalmi egyezéséért felelős személy neve;

d) a másolatkészítő rendszer, illetve a másolatkészítési szabályzat pontos megnevezése és verziószáma;

e) a másolatkészítés időpontja;

f) az irányadó másolatkészítési rend elérhetősége.

(3) A szolgáltató másolatkészítés során tartalmi megfelelés helyett véletlenszerű mintavételezésen alapuló ellenőrzést nem alkalmazhat.

(4) A szolgáltató a szolgáltatás során az igénybevevő elektronikus ügyintézést biztosító szerv adatfeldolgozójaként jár el.

Elektronikus irat hiteles papíralapú irattá alakítása

122. § (1) Az elektronikus irat hiteles papíralapú irattá alakítását az elektronikus ügyintézést biztosító szerv, valamint a Kormány által kijelölt szervezet jelen alcím rendelkezései szerint végezheti.

(2) Ha az elektronikus dokumentum papír alapon történő hiteles megjelenítésének műszaki feltételei adottak, a másolatban rögzíteni kell:

a) az elektronikus dokumentum szöveges és ábrázolt tartalmát,

b) kiadmányozott dokumentum esetén záradékban az eredeti iratot kiadmányozó személy, valamint az elektronikus ügyintézést biztosító szerv nevének és az aláírás időpontjának szöveges megjelenítését, elektronikus bélyegzővel ellátott elektronikus dokumentum esetén a bélyegzőhöz tartozó tanúsítvány szerint a bélyegző létrehozóját meghatározó adatokat,

c) záradékban az elektronikus dokumentum azonosítására vagy a másolat készítésére vonatkozó azon adatokat, amelyek az *a)* pont szerinti tartalomból nem állapíthatóak meg, de a másolatot kérő erre vonatkozóan megfelelő adatot szolgáltatott,

d) „az elektronikus dokumentumban foglaltakkal egyező tartalmú irat” záradékszöveget,

e) a papíralapú másolat keltezését,

f) a másolat hitelesítésének módja szerint a másolatkészítő szervezet elnevezését és a másolatkészítésért felelős, a másolat hitelesítésére jogosult személy aláírását és bélyegzőlenyomatát, az iratérvényességi nyilvántartás szabályai szerinti hitelesítését vagy a (4) bekezdés szerinti hitelesítésre történő utalást.

(3) Ha az elektronikus dokumentum jellemzőire tekintettel arról papíralapú másolat nem készíthető, vagy a készített papíralapú másolat nem tartalmazza az elektronikus dokumentum teljes tartalmát, a másolatot készítő elektronikus ügyintézést biztosító szerv - ha az műszakilag megvalósítható - olyan papíralapú kivonatot készít az elektronikus dokumentumról, amely hivatalos felhasználásra alkalmas. A másolatot készítő elektronikus ügyintézést biztosító szerv ilyen esetben más elektronikus ügyintézést biztosító szerv vagy az ügyfél számára biztosítja az elektronikus dokumentum megismerését.

(4) A papíralapú másolat úgy is elkészíthető, hogy a szolgáltató a teljes, hitelesített elektronikus dokumentumot elhelyezi a papíralapú másolaton, az adatok elektronikus leolvashatóságát biztosító kód formájában. A papíralapú másolat e kód alapján hiteles, ha a kód alapján visszaállított eredeti elektronikus dokumentum megegyezik a papíralapú másolattal.

(5) A másolatkészítő a másolat elkészítését megelőzően köteles ellenőrizni azt, hogy az eredeti elektronikus irat az aláírás és a másolatkészítés időpontja között megváltozott-e, továbbá, hogy az aláírás időpontjában az azt hitelessé tevő tanúsítvány érvényes volt-e. A (2) bekezdés *c)* pontja szerinti adatok tartalmazzák a sértetlenség ellenőrzését igazoló, valamint a hitelesség ellenőrzését lehetővé tevő információkat.

123. § Elektronikus irat hiteles papíralapú irattá alakítása szolgáltatást olyan szervezet végezhet, amely teljesíti az alábbi személyi követelményeket:

a) a másolatkészítésért felelős személy büntetlen előéletű, és

b) a szolgáltató által bevezetett ellenőrzési rendszerben a szolgáltató szabályzata szerint független ellenőr végzi a másolatkészítés szabályszerűségének ellenőrzését.

124. § (1) A másolat automatikusan is elkészíthető, ha

a) a másolatkészítés zárt rendszerben történik, amelynek külső beavatkozástól mentes, az eredeti és a másolat összerendelését tekintve garantáltan hibamentes működését auditálás igazolja,

b) a másolatkészítő rendszer megfelelő műszaki és szervezési megoldással biztosítja a másolat olvashatóságát és a mintavételezésen alapuló minőségbiztosítást.

(2) Automatikus másolatkészítés esetén a dokumentumonkénti tartalmi ellenőrzés helyett véletlenszerű mintavételezésen alapuló ellenőrzés is alkalmazható.

(3) Automatikus másolatkészítés esetén a záradék tartalmazza az automatikus másolatkészítés tényét.

125. § Az egységes kormányzati ügyiratkezelő rendszerből történő irattovábbítás során az elektronikus irat hiteles papíralapú irattá alakítása esetén a szolgáltató a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. részére is biztosítja a másolatkészítés során a technikai ellenőrzés lehetőségét.

126. § (1) A szolgáltató általános szerződési feltételeiben vagy szolgáltatási szabályzatában köteles rögzíteni az elektronikus dokumentum átvételének, a másolatkészítésnek a rendjét, valamint a másolatkészítés teljesítésének feltételeit. A másolatkészítés vállalt határideje legfeljebb 1 munkanap lehet, és - ha az elektronikus irat hiteles papíralapú irattá alakítását megrendelő elektronikus ügyintézést biztosító szerv vagy ügyfél a papíralapú másolat postai küldeményként való feladását igényli - a szolgáltatónak a papíralapú másolatot az elkészítését követő munkanapon postára kell adnia.

(2) A szolgáltató általános szerződési feltételeiben, illetve a hatósággal kötött megállapodásában köteles szabályozni a másolatkészítésre átvett elektronikus dokumentumokkal kapcsolatos teendőit.

(3) A szolgáltató a szolgáltatás során az igénybevevő elektronikus ügyintézést biztosító szerv adatfeldolgozójaként jár el.

Központi Azonosítási Ügynök

127. § (1) A KAÜ KEÜSZ keretében a szolgáltató az elektronikus ügyintézést biztosító szerv számára elérhetővé teszi a vele együttműködő azonosítási szolgáltatásokat, ideértve

a) az azonosítási mód azonosítandó személy általi megválasztásának lehetővé tételét,

b) az azonosítandó személy által kiválasztott azonosítási szolgáltatónál a konkrét azonosítás szükség szerinti végrehajtatását.

(2) A KAÜ KEÜSZ-ön keresztül elérhető legalább

a) valamennyi, a Kormány által kötelezően nyújtott azonosítási szolgáltatás,
b) az elektronikus azonosítási SZEÜSZ-ök, valamint
c) az eIDAS rendelet 6. cikk (1) bekezdése szerinti feltételeknek megfelelő elektronikus azonosítás.

(3) A KAÜ KEÜSZ igénybevételével történő azonosítás során szükség szerint

a) az ügyfél a KAÜ KEÜSZ által elérhetővé tett lehetőségek közül az igénybe venni kívánt azonosítási módot megválasztja,
b) az ügyfél az általa megválasztott módon azonosítja magát,
c) a KAÜ szolgáltatója megadja az azonosítást kérő felé az eIDAS rendelet és az ügyfél hozzájárulása alapján az azonosítási szolgáltató által átadott adatokon kívül az azonosítás eredményeképpen megkapott azonosítót, vagy jelzi az azonosítás sikertelenségét az azonosítást kérőnek,
d) a KAÜ szolgáltatója, ha az ügyfél ügyintézési rendelkezésében erre feljogosította, és az azonosítást kérő ezt igényli, az összerendelési nyilvántartás, a rendelkezési nyilvántartás és az egyedi azonosítást nyilvántartó szerv adatszolgáltatása alapján az azonosítást kérőnek az igényelt egyedi leíró adatokat (a továbbiakban: attribútum), illetve az annak megfelelő összerendelési nyilvántartásban szereplő bejegyzés elemet, illetőleg az összerendelési nyilvántartás szolgáltatója ügynöki szolgáltatása révén megkapott leíró adatokat (a továbbiakban: attribútum) adja meg.

(4) A KAÜ szolgáltatója felel az általa nyújtott azonosítási mozzanatok és kapcsolódó szolgáltatások megfelelőségéért. A szolgáltatás nyújtása során az elektronikus azonosítás igénybevétele esetén az azonosítás megfelelőségéért az azonosítási szolgáltató felel.

(5) A KAÜ szolgáltatója az azonosítást kérő felé megadhatja a képviseleti jogosultságra vonatkozó információkat az ehhez szükséges, 94. § (4) bekezdés szerinti ügynöki szolgáltatás révén.

Személyre szabott ügyintézési felület

128. § (1) A személyre szabott ügyintézési felület (a továbbiakban: SZÜF) KEÜSZ-t az ügyfelek 127. § (2) bekezdése szerinti elektronikus azonosítóeszközök használata mellett vehetik igénybe.

(2) A SZÜF-ön keresztül elérhető elektronikus ügyintézési szolgáltatások szolgáltatói - a (3) bekezdésben meghatározott kivétellel - az ügyfélnek a saját szolgáltatásuk megkezdéséhez szükséges azonosításához elfogadják a SZÜF-re történő belépéskor alkalmazott azonosítást.

(3) Ha az elektronikus ügyintézési szolgáltatás szolgáltatója a SZÜF-re történő belépéskor alkalmazottnál magasabb biztonsági szintű azonosítóeszköz használatát követeli meg, az elektronikus ügyintézési szolgáltatás használatának megkezdésekor kötelezheti az ügyfelet a magasabb biztonsági szintű azonosítóeszköz alkalmazására.

(4) A SZÜF-ön elérhető SZEÜSZ vagy KEÜSZ szolgáltatója részére, valamint az igénybe vett elektronikus ügyintézési szolgáltatást nyújtó elektronikus ügyintézést biztosító szerv részére, erre irányuló kérésük esetén a SZÜF szolgáltatója az azonosítási szolgáltató által rendelkezésre bocsátott adatot azonosítási célból elérhetővé teszi.

(5) A (4) bekezdés szerinti eseten kívül SZEÜSZ vagy KEÜSZ szolgáltató, illetve elektronikus ügyintézést biztosító szerv az érintett adatok szolgáltatását az ügyféltől csak akkor kérheti, ha a SZÜF szolgáltatója által rendelkezésre bocsátott adatok valóságtartalma tekintetében kétsége merül fel, vagy annak igazolását jogszabály előírja.

(6) Az (5) bekezdés szerinti korlátozás nem terjed ki a szolgáltató azon azonosítás kéréseire, amikor biztonsági megfontolásból szükséges az ügyfél ismételt azonosítása, függetlenül annak biztonsági szintjétől.

Elektronikus dokumentumtárolási szolgáltatás

129. § (1) Az elektronikus dokumentumtárolási szolgáltatás (a továbbiakban: EDT) KEÜSZ önállóan nyújtható részszolgáltatása

a) az átmeneti tárolás, ahol a szolgáltató a tárolásra használt megoldás technológiai korlátaiból adódó kockázat figyelembevételével meghatározza a megőrzés vállalt leghosszabb idejét,

b) az elektronikus irattári szolgáltatás, valamint

c) a tartós tárolás, ahol a szolgáltató köteles gondoskodni a tárolási technológia korlátai miatt a dokumentum tárolásának szükség szerinti megújításáról.

(2) A közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló kormányrendelet hatálya alá tartozó elektronikus ügyintézést biztosító szerv részére nyújtott, az (1) bekezdés *b)* pontja szerinti szolgáltatás esetén az EDT szolgáltatója a tárolt dokumentumokhoz kapcsolódó egyes iratkezelési műveleteket is elvégezheti, ennek részeként

a) a tárolásra átvételt és a visszaadást az iratformátumokra, az ott előírt járulékos kísérő és metaadatokra is kiterjedően, az irattári kezelés szabályai szerint végezheti,

b) a tárolt iratok levéltárba adását és selejtezését az elektronikus ügyintézést biztosító szerv konkrét rendelkezése alapján elvégezheti, valamint

c) a tárolást a levéltári kezelés dokumentummegőrzési informatikai szolgáltatási hátterére vonatkozó szabályok szerint is biztosíthatja.

(3) Ha a szolgáltató az EDT-t több elektronikus ügyintézést biztosító szerv részére is nyújtja, az iratok tárolását köteles elkülönítetten végezni.

(4) Az elektronikus dokumentum tartós tárolásra történő átvételekor a szolgáltató ellenőrzi az elektronikus dokumentum hitelesítésének érvényességét. Az elektronikus okirat kiadásakor a

szolgáltató elektronikus bélyegzővel hitelesíti az elektronikus dokumentumot. Az így hitelesített elektronikus dokumentum változatlanságát - ha az elektronikus bélyegző ellenőrzésének eredményéből más nem következik - vélelmezni kell.

(5) Ha a tartós tárolásra átvett elektronikus dokumentum dokumentumformátuma miatt az elektronikus dokumentum megnyithatósága nem biztosítható, a szolgáltató jogosult az elektronikus dokumentum más dokumentumformátumba alakítására. A szolgáltató az átalakított dokumentumot záradékolja, feltüntetve a formátumváltás tényét, idejét, a készítő nevét vagy gépi szolgáltatás igénybevétele esetén azonosítóját, valamint az eredeti irat hitelesítésével kapcsolatos információkat. A szolgáltató az átalakított elektronikus dokumentumot a záradékkal együtt elektronikus bélyegzővel hitelesíti.

130. § (1) A szolgáltató - a vonatkozó jogszabályi rendelkezéseket figyelembe véve - meghatározhatja azokat a formátumokat, amelyekben az elektronikus dokumentumokat átveszi és tárolja. Jogszabály meghatározhatja azon formátumokat, amelyeket a szolgáltató tárolásra átvenni köteles.

(2) A tárolásra átvett dokumentumokon bármilyen fajta, nem technikai jellegű keresési vagy összekapcsolási művelet csak az adott adatkörre, az elektronikus ügyintézést biztosító szerv által adott ilyen irányú kifejezett hozzájárulás alapján végezhető.

(3) A szolgáltató köteles biztosítani

a) az egyes dokumentumok egyértelmű azonosítottságát,
b) az átvett dokumentumokon végzett valamennyi műveletnek olyan megoldással történő naplózását, amely az utólagos észlelhetetlen módosítás lehetőségét kizárja, valamint
c) az iratok átvételének és visszaadásának az elektronikus iratok kezelésére vonatkozó szabályoknak megfelelő dokumentálását.

Iratkezelő rendszerek közötti iratáthelyezés

131. § (1) Az iratkezelő rendszerek közötti iratáthelyezés KEÜSZ keretében az elektronikus felületen átadott, elektronikus iktatókönyvben nyilvántartott irat, ügyirat, irategyüttes (ezen alcím alkalmazásában a továbbiakban együtt: irat) akkor minősül átadottnak, amikor a szolgáltató - az átvevő elektronikus ügyintézést biztosító szerv rendszerének elektronikus értesítése mellett - az átvevő elektronikus ügyintézést biztosító szerv számára elérhetővé teszi

a) az iratot elektronikus formában, valamint
b) az elektronikus iktatókönyv iratra vonatkozó iktatási adatait.

(2) Az iratáthelyezésről a címzett elektronikus ügyintézést biztosító szerv az iratkezelési rendszerén keresztül igazolást ad a szolgáltató részére, amely igazolást vagy - annak 3 napon túli elmaradása esetén - az iratáthelyezés sikertelenségéről szóló, a szolgáltató által kiállított igazolást a szolgáltató az átadást kezdeményező elektronikus ügyintézést biztosító szervnek megküldi.

(3) Az iratot átadó elektronikus ügyintézést biztosító szerv az iratáthelyezés megtörténtére vonatkozó (2) bekezdés szerinti igazolás átvételét követően az iratáthelyezés sikerességét iratkezelő rendszerében rögzíti.

(4) Az iratot átvevő elektronikus ügyintézést biztosító ellátó szerv az átvett iratot az elektronikus iratkezelő rendszer átadott adatai alapján a saját iratkezelő rendszerében - ha ezt az iratáthelyezésben érintett elektronikus ügyintézést biztosító szerv iratkezelési szabályzata lehetővé teszi, automatikus iktatás útján - elhelyezi.

(5) Az elektronikus iktatórendszernek az irattal együtt továbbított adatait az iratot átvevő elektronikus ügyintézést biztosító szerv által közvetlenül értelmezhető formában kell az irathoz mellékelni.

Központi dokumentumhitelesítési ügynök

132. § (1) A központi dokumentumhitelesítési ügynök (a továbbiakban: KDÜ) KEÜSZ keretében a szolgáltató az ügyfél és az elektronikus ügyintézést biztosító szerv számára elérhetővé teszi dokumentumhitelesítési szolgáltatások használatát, ideértve

a) valamely dokumentum hitelesítését a kiválasztott dokumentumhitelesítéssel, ideértve legalább az azonosításra visszavezetett dokumentumhitelesítés KEÜSZ használatát és az elektronikus aláírással vagy elektronikus bélyegzővel történő hitelesítést,
b) a hitelesített dokumentum biztonságos kézbesítési szolgáltatás útján e rendelet szerinti elektronikus tárhelyre történő továbbítását és
c) az igénybevevő által megjelölt adaton vagy dokumentumon elhelyezett elektronikus aláírás vagy bélyegző érvényességének ellenőrzését, valamint
d) az ellenőrzés eredményéről igazolás kiállítását.

(2) A szolgáltató biztosítja, hogy a szolgáltatást igénybe vevő ügyfél vagy elektronikus ügyintézést biztosító szerv az elektronikus aláírás vagy bélyegző létrehozásához szükséges magánkulcsot a szolgáltatáson belül biztonságosan tárolja, és megfelelő azonosítás után a tárolt magánkulcs használatával hitelesítse az elektronikus dokumentumot.

(3) A szolgáltató biztosítja, hogy az elektronikus ügyintézést biztosító szervek a KDÜ KEÜSZ-ön keresztüli automatizált dokumentumhitelesítési megoldást is alkalmazhassanak.

(4) A KDÜ szolgáltatója az általa nyújtott hitelesítési mozzanatok és kapcsolódó szolgáltatások megfelelő elérhetővé tételéért felel.

Összerendelési nyilvántartás

134. § (1) Az összerendelési nyilvántartás KEÜSZ szolgáltatója összerendelési nyilvántartást vezet a személyiadat- és lakcímnyilvántartásban, a központi idegenrendészeti nyilvántartásban, valamint az elektronikus ügyintézést igénybe vevő, külföldön élő természetes személyek személyi nyilvántartásában szereplő valamennyi élő természetes személyre vonatkozóan (a továbbiakban: természetes személyek összerendelési nyilvántartása).

(2) Az (1) bekezdésben meghatározott nyilvántartásokban kezelt adatok változásáról, így különösen az érintett személy haláláról nyilvántartást vezető szervek értesítik az összerendelési nyilvántartást kezelő szervet.

(3) A természetes személyek összerendelési nyilvántartásából a természetes személyt

a) halála,
b) magyar állampolgárságának megszűnése,
c) nem magyar állampolgár magyarországi tartózkodási státuszának megszűnése

esetén, az erre vonatkozó tény közhiteles nyilvántartásába történő bejegyzését követő 5 éven belül törölni kell.

(4) Az összerendelési nyilvántartáshoz csak a felügyelet által kiadott ajánlásban meghatározott programozott felületen lehet hozzáférést biztosítani.

(5) Az összerendelési nyilvántartásból csak előzetesen regisztrált szervezetek számára, kizárólag automatizált interfész útján, a jogosultságuk ellenőrzését követően, a jogosultságuknak megfelelő adatokra vonatkozóan szolgáltatható adat.

(6) Az összerendelési nyilvántartásból történő adatszolgáltatás

a) időpontját,
b) az érintett azonosításához szükséges adatokat,
c) a szolgáltatott adatok megjelölését,
d) az adatszolgáltatás címzettjét,
e) az adatszolgáltatás címzettjének jogosultságát megalapozó jogszabályi rendelkezést és az adatszolgáltatás célját

naplózni kell.

(7) A természetes személyek összerendelési nyilvántartásából az arra jogosult személy részére az általa jogszerűen kezelt, természetes személyre vonatkozó titkosított kapcsolati kód alapján a kérelemben megjelölt nyilvántartásban szereplő ugyanazon természetes személy titkosított kapcsolati kódja szolgáltatható.

(8) Az összerendelési nyilvántartás KEÜSZ szolgáltatója attribútum szolgáltatási ügynöki szolgáltatásként a (7) bekezdésben meghatározott szolgáltatáson túl az elektronikus ügyintézést biztosító szerv részére az alábbi szolgáltatásokat nyújthatja:

a) az arra jogosult részére az általa jogszerűen kezelt, természetes személyre vonatkozó titkosított kapcsolati kód alapján a természetes személy természetes személyazonosító adatainak szolgáltatása, az érintett nyilvántartásokat kezelő szervek bevonásával,
b) egy egyedi azonosítóhoz tartozó más nyilvántartásban alkalmazott egyedi azonosító vagy a természetes személyazonosító adatok szolgáltatása, a természetes személy egyedi vagy az ügyintézési rendelkezések nyilvántartásában rögzített hozzájárulása alapján,
c) az elektronikus ügyintézést biztosító szerv által jogszerűen kezelt, természetes személyre

vonatkozó titkosított kapcsolati kód alapján az ügyintézési rendelkezését leíró attribútumok szolgáltatása, az érintett nyilvántartást kezelő szerv bevonásával.

(9) Az attribútum szolgáltatási ügynöki szolgáltatást igénybe vevő szerv az összerendelési nyilvántartás szolgáltatója részére a szolgáltatás igénybevétele céljának megjelölésével egyidejűleg igazolni köteles

a) az érintett adatok kezelésének jogszerűségét a vonatkozó jogszabályi rendelkezés megjelölésével, vagy
b) az ügyfél hozzájárulását az azonosított ügyfél ügyintézésének lefolytatásához szükséges leíró attribútumainak kezeléséhez.

(10) Az attribútum szolgáltatási ügynöki szolgáltatás

a) közvetlen szolgáltatáseléréssel vagy
b) elektronikus ügyfélazonosítás esetén - közvetetten a KAÜ KEÜSZ szolgáltatáson keresztül érhető el.

(11) A (10) bekezdés *b)* pontja szerinti esetben az igénybevevő a választott azonosítási módtól függő azonosító adattal igényelheti az érintett ügyfél attribútumait.

V. FEJEZET
AZ ELEKTRONIKUS ÜGYINTÉZÉSI FELÜGYELET

26. A felügyelet eljárására és a felügyeleti vizsgálatra vonatkozó részletes szabályok

135. § A felügyelet feladata:

a) a SZEÜSZ-ökre és KEÜSZ-ökre vonatkozó jogszabályok megalkotásának, módosításának kezdeményezése;
b) az elektronikus ügyintézést érintő jogszabálytervezetek véleményezése;
c) a SZEÜSZ-ök, KEÜSZ-ök, az elektronikus ügyintézési szolgáltatások, az elektronikusan intézhető ügyek és az elektronikus ügyintézést biztosító szervek nyilvántartása;
d) a SZEÜSZ-ök és KEÜSZ-ök ellenőrzése;
e) a hozzá érkező bejelentések kivizsgálása;
f) az elektronikus ügyintézést biztosító szervek az E-ügyintézési tv.-ben meghatározott kötelezettségei teljesítésének ellenőrzése;
g) az információforrások regiszterének, az adat- és iratmegnevezések jegyzékének a vezetése;
h) az információátadási szabályzatok és információátadási megállapodások bejelentésének fogadása;
i) műszaki irányelvek elfogadása;
j) az együttműködő szervek az E-ügyintézési tv.-ben szabályozott tevékenységeinek felügyelete.

136. § (1) A felügyelet ellenőrzi, hogy a szolgáltató és az elektronikus ügyintézést biztosító szerv az elektronikus ügyintézéssel kapcsolatos jogszabályban, foglalt követelményeknek megfelel-e, a szolgáltató a nyilvánosságra hozott tájékoztatóiban és általános szerződési feltételeiben foglaltakat, valamint - ha van ilyen - szerződési feltételeit betartja-e, valamint ellenőrzi a felügyelet korábbi döntéseinek végrehajtását.

(2) A felügyelet az E-ügyintézési tv. 48. § (2) bekezdése szerinti intézkedés megtétele során figyelembe veszi a megállapított mulasztásnak az ügyfelekre és az érintett szervek működésére, továbbá intézkedésének az ügyfelekre gyakorolt hatását, valamint - adott esetben - más szolgáltatásra való átállás lehetőségét, annak költségét és időigényét.

(3) Az elektronikus ügyintézést biztosító szerv az E-ügyintézési tv. 28. § (1) bekezdése szerint a következő adatokat köteles bejelenteni a felügyeletnek:

a) nevét, székhelyét, hivatalos elektronikus elérhetőségét;
b) kapcsolattartójának nevét és elektronikus elérhetőségét, ha a kapcsolattartó az adatai kezeléséhez hozzájárult;
c) azon ügyfajtákat, amelyekben az elektronikus ügyintézés lehetőségét biztosítja, és ennek kezdő időpontját, valamint
d) az általa nyújtott elektronikus ügyintézéssel kapcsolatos szolgáltatások megnevezését.

136/A. § (1) Az E-ügyintézési tv. 48. § (2) bekezdése szerinti esetben a felügyelet - a jogsértés mértékétől függően, a jogsértés által okozott kár és joghátrány figyelembevételével - a bírság mértékét a következők szerint állapíthatja meg:

a) a bírság mértéke tízezertől ötszázezer forintig terjedhet, ha a jogsértés csak egy ügyfelet érintett, akinek a jogsértésből jelentős hátránya nem származott;
b) a bírság mértéke ötszázezertől ötmillió forintig terjedhet, ha a jogsértés
ba) több ügyfelet érintett,
bb) az érintett ügyfélnek a jogsértésből jelentős hátránya származott, vagy
bc) a felügyelet az elektronikus ügyintézést biztosító szervet az *a)* pont szerinti jogsértés miatt egy éven belül már megbírságolta;
c) a bírság mértéke ötmillió forinttól ötvenmillió forintig terjedhet, ha
ca) a felügyelet az elektronikus ügyintézést biztosító szervet a *b)* pont szerinti jogsértés miatt egy éven belül már megbírságolta,
cb) a jogsértés miatt az ügyfél személyes adatait arra jogosulatlan szerv vagy személy megszerezte, vagy
cc) a jogsértés több ügyfélnek jelentős hátrányt okozott.

(2) A felügyelet az E-ügyintézési tv. 48. § (2) bekezdése szerinti jogkövetkezmények alkalmazása esetében - az E-ügyintézési tv. 48. § (2) bekezdés *d)* pontja szerinti eset kivételével - ismételt ellenőrzéssel köteles meggyőződni az intézkedés eredményességéről, a jogszabálysértésnek az elektronikus ügyintézést biztosító szerv általi megszüntetéséről.

28. A szolgáltatásnyújtás bejelentése

138. § (1) A KEÜSZ vagy SZEÜSZ szolgáltató köteles a felügyelet részére a szolgáltatás nyújtásának megkezdésére irányuló szándékot, valamint a megkezdés tervezett időpontját elektronikusan, a felügyelet által közétett tájékoztatás szerint bejelenteni.

(2) A szolgáltató a bejelentéshez köteles csatolni:

a) a szolgáltatás részletes műszaki leírását,
b) a szolgáltatás pontos meghatározásához szükséges eljárási, adminisztrációs szabályokat, szabályzatokat, folyamatleírásokat, hitelesítési rendet, ahol az értelmezett,
c) a szolgáltatásra vonatkozó általános szerződési feltételeket,
d) a szolgáltató katasztrófaelhárítási eljárásra vonatkozó szabályzatát,
e) a külön jogszabályban meghatározott biztonsági és egyéb műszaki követelményeknek való megfelelést alátámasztó dokumentumokat, valamint
f) a független tanúsító szerv által kiadott, jogi, informatikai minőségügyi és informatikai biztonsági vizsgálat alapján készült teljes körű jogi és informatikai audit jelentést.

(3) A bejelentés szükség esetén intézkedési tervet tartalmaz, amelyben foglaltak teljesülését a felügyelet ellenőrzi.

(4) A felügyelet megkeresése alapján a szolgáltatás nyilvántartásba vételére vonatkozó eljárásban a szolgáltatás információbiztonságának véleményezése érdekében a bejelentést a Nemzeti Elektronikus Információbiztonsági Hatóság - a megkereséstől számított 8 napon belül - véleményezi.

(5) A felügyelet - ha a nyilvántartásba vétel megtagadásának indoka nem áll fenn - a szolgáltatót a bejelentésben közölt adatoknak megfelelően bejegyzi a szolgáltatókról vezetett nyilvántartásába, és - ha hiánypótlás nem szükséges - a bejelentés időpontjától számított 8 napon belül a nyilvántartásba vétel tényét visszaigazolja.

(6) A felügyelet megtagadja a nyilvántartásba vételt, ha

a) a bejelentésben foglalt adatok a hiánypótlás ellenére a szolgáltató vagy az általa végezni kívánt tevékenység azonosítására, illetve a nyilvántartásba vételre nem alkalmasak,
b) a szolgáltatás nyújtása a benyújtott információk alapján nem alkalmas a biztonságos igénybevételhez.

(7) A szolgáltató a bejelentésben közölt adatokban bekövetkezett változásokat, valamint a szolgáltatás nyújtásának megszűnését 30 napon belül köteles bejelenteni a felügyeletnek.

(8) A felügyeletnek a szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól szóló törvény szerinti, a szolgáltatókról szóló nyilvántartását a felügyelet a honlapján közzéteszi, és abba bárki betekinthet.

(9) A felügyelet vizsgálata kiterjed

a) a műszaki követelmények,
b) az eljárási feltételek,
c) a biztonsági követelmények,
d) a szolgáltatási feltételek,
e) az *a)* és *d)* pontok teljesülését garantáló szolgáltatási képesség,
f) a szolgáltatáshoz kapcsolódó járulékos feltételeknek való megfelelés és
g) a szolgáltatás jogszabályoknak való megfelelése

vizsgálatára.

(10) Ha a (9) bekezdés szerinti valamely követelményre rendelkezésre áll a felügyelet által közzétett ajánlás, és a szolgáltató az ajánlás alkalmazásáról nyilatkozik, a felügyelet az ellenőrzés során az ajánlásban rendezett kérdésekben kizárólag az ajánlásnak való megfelelést ellenőrzi.

(11) A szolgáltató a szolgáltatásnyújtás megkezdésének tervezett időpontját köteles a bejegyzés iránti kérelem benyújtását követő 3 hónapon túli időpontban megjelölni.

138/A. § A szolgáltató által benyújtott szolgáltatási szabályzat legalább a 64. § (3) bekezdése szerinti információkat tartalmazza.

140. § (1) A felügyelet a jogszabályban foglalt követelményeknek való megfelelés vizsgálata során mérlegelési jogkörében figyelembe veszi az érintett szolgáltatásra irányadó műszaki előírásokat és a kérelemben foglalt szolgáltatás egyedi sajátosságait.

(2) A felügyelet a jogszabályban foglalt követelményeknek való megfelelés vizsgálata során helyszíni szemlét is lefolytathat, és kérheti a szolgáltatás műszaki jellemzőinek, működésének részletes bemutatását.

(3) A felügyelet döntésében köteles a figyelembe vett műszaki előírásokat nevesíteni, és ha a szolgáltatásra irányadó műszaki előírásoktól eltért, köteles az eltérést megindokolni.

142. § A felügyelet a bizalmi szolgáltatásnak is minősülő SZEÜSZ és KEÜSZ szolgáltatások ellenőrzése tekintetében minden esetben egyeztet az E-ügyintézési tv. 91. § (1) bekezdése szerinti bizalmi felügyelettel. A felügyelet nem vizsgálja a szolgáltatásnak a bizalmi szolgáltatásokra vonatkozó jogszabályoknak való megfelelőségét.

29. A szolgáltatásnyújtás megszüntetése

143. § (1) A szolgáltató köteles a felügyelet részére a szolgáltatás nyújtásának megszüntetése előtt legalább 90 nappal a szolgáltatás befejezését bejelenteni, és azt az elektronikus tájékoztatás szabályai szerint közzétenni.

(2) A bejelentés nem mentesíti a szolgáltatót a megállapodások alapján vállalt vagy jogszabály által kötelezően előírt szolgáltatási időszak biztosításától.

(3) Ha a szolgáltatás nyújtását nem jogszabály írja elő kötelezően, a felügyelet jogosult a szolgáltatás megszüntetésének idejét legfeljebb 6 hónappal elhalasztani, ha a szolgáltatás

nyújtásának megszüntetése az elektronikus ügyintézés során zavarokat okozhat. A szolgáltató - ha a szolgáltatást nem jogszabályi kötelezés alapján nyújtja - mentesülhet e szolgáltatási kötelezettsége alól, ha teljes értékűen azonos, a felügyelet nyilvántartásában szereplő szolgáltatás az igénybevevők rendelkezésére áll, az átállásra elegendő időt biztosít, és az igénybevevők esetleges átállási költségét a tevékenységét megszüntető szolgáltató viseli.

30. A koordinációs eljárás részletes szabályai

144. § (1) A koordinációs eljárás a felügyelet speciális, az elektronikus ügyintézést biztosító, illetve az együttműködő szervet szakmailag segítő, e szerv kérelmére vagy hivatalból indítható eljárása, amely nem minősül közigazgatási hatósági eljárásnak.

(2) A felügyelet a koordinációs eljárás során javaslatainak előkészítése érdekében információkat kér az elektronikus ügyintézést biztosító vagy együttműködő szervtől, az érintett szervekkel konzultációt folytat, a helyszínen felméri az E-ügyintézési tv. és e rendeletben foglalt feltételek teljesüléséhez szükséges adatokat.

(3) A felügyelet munkatársai a koordinációs eljárás során tudomásukra jutott információkat a (4) bekezdés szerinti kivétellel kötelesek bizalmasan kezelni.

(4) Ha a felügyelet a koordinációs eljárás során olyan információ birtokába jut, amely információbiztonsági kockázatot jelenthet, haladéktalanul értesíti az elektronikus információs rendszerek biztonságának felügyeletéért felelős hatóságot.

(5) Az elektronikus ügyintézést biztosító vagy együttműködő szerv - a Kormány rendeletében meghatározott kivételekkel - nem köteles a felügyelet javaslatában foglaltak végrehajtására, de jeleznie és indokolnia kell a felügyeletnek a javaslatban foglaltaktól történő eltérést.

(6) A felügyelet a koordinációs eljárás eredményéről összefoglalót készít, amelyet az elektronikus ügyintézést biztosító vagy együttműködő szervnek megküld.

39. Az Európai Unió jogának való megfelelés

156. § Ez a rendelet a belső piaci szolgáltatásokról szóló, 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelv 6−8. cikkeinek, valamint az illetékes hatóságok által a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti és tanácsi irányelv alapján elektronikusan aláírt dokumentumok országhatáron átnyúló feldolgozására vonatkozó minimumkövetelményekről szóló 2011/130/EU határozat módosításáról szóló 2014/148/EU bizottsági végrehajtási határozatban meghatározott szabványformátumokra vonatkozó rendelkezéseknek való megfelelést szolgálja.

1. melléklet a 451/2016. (XII. 19.) Korm. rendelethez

Az elektronikus ügyintézést biztosító szervek által kötelezően elfogadott elektronikus dokumentumformátumok

A dokumentum jellege	Fájlkiterjesztés	Alapul vett szabvány
formázás nélküli szöveg	.txt	
szöveges dokumentum (formázással), beágyazott képpel vagy más információval	.pdf	ISO 32000-1:2008 ISO 19005-1:2005
szöveges dokumentum (formázással), beágyazott képpel vagy más információval	.docx	ISO/IEC 29500-1:2016
szöveges dokumentum (formázással), beágyazott képpel vagy más információval	.odt	ISO/IEC 26300:2006 ISO 26300-1:2015
táblázat	.xlsx	ISO/IEC 29500-1:2016
táblázat	.ods	ISO/IEC 26300:2006 ISO 26300-1:2015
tömörítetlen kép	.tif, .tiff	ISO 12639:2004
tömörített kép	.jpg, .jpeg	ISO/IEC 10918-1:1994
ábra	.png	ISO/IEC 15948:2004
videó	.mp4, .m4a	ISO/IEC 14496-10:2003 ISO/IEC 14496-14:2003
videó	.mpeg, .mpg	ISO/IEC 13818
hang	.mp3	MPEG-1: ISO/IEC 11172-3
hang	.wav	

2. melléklet a 451/2016. (XII. 19.) Korm. rendelethez

A piaci szereplő részére biztosított SZEÜSZ/KEÜSZ szolgáltatásért fizetendő díj megállapításának szabályai

1. A Szolgáltató - a 2. pontban megjelöltek kivételével - a szolgáltatásaiért havonta fizetendő díjat (a továbbiakban: havi díj) havi alapdíj (a továbbiakban: havi alapdíj) és a szolgáltatás darabja vagy a szolgáltató által meghatározott adatforgalmi mennyiségi egység igénybevételének havi tételszáma alapján határozza meg (a továbbiakban: egységdíj), a szolgáltatások egységdíja, valamint a szolgáltatások havi tételszáma szorzatának és a havi alapdíjnak az összegeként.

2. A Kormány által kijelölt szolgáltató tranzakciós díjat - melyben jogszabályban biztosított észszerű nyereséget is megállapít - számol fel az adott szolgáltatás igénybevételi tranzakció száma és a tranzakció egységdíjának szorzata alapján.

137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről

http://njt.hu/cgi_bin/njt_doc.cgi?docid=195858.342128

A Kormány az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 105. § (1) bekezdés *g)* pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

1. Általános rendelkezések

1. § (1) E rendelet hatálya - a (2) és (3) bekezdésben foglalt kivétellel -

a) az elektronikus ügyintézési szolgáltatások nyújtására használható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó tanúsítvány alanyára, valamint az annak képviseletében eljáró személyre,
b) az elektronikus ügyintézést biztosító szervre,
c) az elektronikus ügyintézési célra használható elektronikus aláírással vagy bélyegzőkkel kapcsolatos bizalmi szolgáltatóra, valamint az ilyen szolgáltatásokat nyújtani kívánókra,
d) a Nemzeti Média- és Hírközlési Hatóságra (a továbbiakban: NMHH)

terjed ki.

(2) A titkos információgyűjtés, valamint titkos adatszerzés eszközei és módszerei alkalmazásában, engedélyezésében részt vevő szervek, valamint személyek e feladatkörükben eljárva, egymás közötti, zárt körben történő elektronikus aláírás vagy bélyegző létrehozását, elfogadását, felhasználását a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendelet (a továbbiakban: eIDAS Rendelet) 2. cikk (2) bekezdése szerint külön megállapodásban szabályozhatják.

(3) A (2) bekezdés szerinti megállapodás alapján nyújtott szolgáltatásokra e rendelet előírásait nem kell alkalmazni.

(4) E rendelet alkalmazásában

1. *közigazgatási gyökértanúsítvány:* a közigazgatási gyökér-hitelesítésszolgáltató által kibocsátott tanúsítvány, amelyben a közigazgatási gyökér-hitelesítésszolgáltató elektronikus bélyegzőjével hitelesíti az elektronikus ügyintézési célra, illetve közigazgatási célra használható elektronikus aláírás- vagy bélyegző tanúsítványára meghatározott követelményeknek megfelelő tanúsítványt kibocsátó bizalmi szolgáltató nyilvános kulcsát és tanúsítja, hogy a tanúsítvány által megjelölt bizalmi szolgáltató az ügyintézési célra felhasználható tanúsítványt bocsát ki;

2. *elektronikus tájékoztatás szabálya:* az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési tv.) felhatalmazása alapján kiadott végrehajtási rendeletekben meghatározott, az elektronikus ügyintézési eljárásokkal kapcsolatos tájékoztatás módjára vonatkozó szabály;

3. *távoli elektronikus aláírás:* nem az elektronikus ügyintézést biztosító szerv hivatali helyiségében, de annak elektronikus ügyintézésével összefüggésben történő elektronikus aláírás.

2. Az e-közigazgatásért felelős miniszternek a közigazgatási gyökér-hitelesítésszolgáltatóval kapcsolatos feladatai

2. § Az elektronikus aláírásra és bélyegzőre vonatkozó jogszabályok, az Európai Unió általános hatályú, közvetlenül alkalmazandó kötelező jogi aktusai, valamint szabványban vagy egyéb követelmények figyelembevételével az NMHH és az e-közigazgatásért felelős miniszter (a továbbiakban: miniszter) rendszeresen, évente legalább egy alkalommal egyeztet arról, hogy a közigazgatási gyökér-hitelesítésszolgáltatónak milyen, a működéshez szükséges szabályozási dokumentumokkal (politikákkal, szabályzatokkal és eljárásrendekkel) kell rendelkeznie.

3. A közigazgatási gyökér-hitelesítésszolgáltató

3. § (1) A közigazgatási gyökér-hitelesítésszolgáltató elektronikus bélyegzőjével hitelesíti az e rendeletben az elektronikus ügyintézést biztosító állami szervek által használt bizalmi szolgáltatáshoz tartozó tanúsítvánnyal szemben meghatározott követelményeknek megfelelő tanúsítványt kibocsátó bizalmi szolgáltató nyilvános kulcsát, és erről közigazgatási gyökértanúsítványt bocsát ki.

(2) A közigazgatási gyökér-hitelesítésszolgáltató az NMHH szervezeti egysége, működtetéséről az NMHH − az e rendeletben meghatározottak szerint - gondoskodik, vezetőjét az NMHH elnöke nevezi ki.

4. § (1) A közigazgatási gyökér-hitelesítésszolgáltatónál a jogszabályban meghatározott bizalmi munkakörök közül önálló munkakört kell létesíteni a biztonsági tisztviselő és a független rendszervizsgáló számára.

(2) A közigazgatási gyökér-hitelesítésszolgáltatót igazoló bélyegző-létrehozó adat előállítását, másolását, megsemmisítését, valamint elektronikus bélyegző létrehozását a közigazgatási gyökér-hitelesítésszolgáltató szabályzatában arra feljogosított személyek együttes részvételével, jogosultsággal nem rendelkező személyek kizárásával kell végezni.

(3) A közigazgatási gyökér-hitelesítésszolgáltató vezetője, valamint az (1) és (2) bekezdésben meghatározott személyek az NMHH köztisztviselői.

(4) Az NMHH elnöke gondoskodik a közigazgatási gyökér-hitelesítésszolgáltató − a gyökér-hitelesítésszolgáltatói feladat ellátásához, a szolgáltatás megbízható és a rá vonatkozó követelményeknek megfelelő működéséhez szükséges − védelmének biztosításáról.

4. Az elektronikus ügyintézési célra, illetve közigazgatási célra használható elektronikus aláírással, elektronikus bélyegzővel és tanúsítványokkal szembeni követelmények

5. § (1) Ha törvény eltérően nem rendelkezik, az E-ügyintézési tv. szerinti ügyekben az elektronikus ügyintézést biztosító szerv olyan elektronikus aláírást vagy bélyegzőt használhat, amely megfelel az e rendeletben meghatározott követelményeknek.

(2) Az elektronikus ügyintézést biztosító szerv a funkcionális működésével összefüggő ügyekben - ha azokkal kapcsolatban az E-ügyintézési tv. alkalmazását vállalta - olyan elektronikus aláírást vagy bélyegzőt használhat, amely megfelel az e rendeletben meghatározott követelményeknek.

6. § Elektronikus ügyintézési célra olyan elektronikus aláírás, elektronikus bélyegző vagy tanúsítvány használható, amely

a) az ügyintézésben közreműködő, kiadmányozásra nem jogosult személy (a továbbiakban: ügyintéző) által használt aláírás esetén a 13. §-ban meghatározott követelményeknek,
b) az ügyintézést biztosító szerv nevében kiadmányozásra feljogosított természetes személy által használt aláírás esetén a 14. §-ban meghatározott követelményeknek,
c) az ügyintézést biztosító szerv számítógépes rendszere által dokumentum- vagy kommunikációhitelesítésre használt bélyegző esetén a 15. §-ban meghatározott követelményeknek

megfelel.

7. § Az elektronikus aláírást vagy bélyegzőt az elektronikus ügyintézést biztosító szerv az 5. § szerinti ügyekben akkor használhatja, ha az legalább fokozott biztonságú, és

a) elektronikus ügyintézést biztosító állami szerv esetén a tanúsítványát olyan bizalmi szolgáltató bocsátotta ki, amelynek nyilvános kulcsát a közigazgatási gyökér-hitelesítésszolgáltató felülhitelesítette,
b) a bizalmi szolgáltató hitelesítési rendje szerint a tanúsítvány kibocsátását megelőző személyazonosítás (a továbbiakban: regisztráció) során - ha e rendelet eltérően nem rendelkezik - a 9. és 10. §-ban foglaltak szerint jár el, és
c) az aláírás vagy bélyegző megfelel a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendelet 27. cikkének (5) bekezdése és 37. cikkének (5) bekezdése szerint a közigazgatási szervek által elismert fokozott biztonságú elektronikus aláírások és fokozott biztonságú bélyegzők formátumaira vonatkozó specifikációk meghatározásáról szóló, 2015. szeptember 8-ai (EU) 2015/1506 bizottsági

végrehajtási határozatban foglalt követelményeknek.

8. § A bizalmi szolgáltató tanúsítvány kibocsátását megelőzően a regisztrációt elvégezheti

a) az eIDAS Rendelet 24. cikk (1) bekezdésében foglalt módon,
b) helyszíni ellenőrzéssel − a 10. §-ban foglalt eltérésekkel - a 9. § szerint,
c) feltételes regisztrációval a 11. §-ban foglaltak szerint, vagy
d) elektronikus ügyintézést biztosító állami szerv esetén annak humánpolitikai szervezete által, az ügyintézést biztosító állami szerv személyzeti nyilvántartására alapozva a 13. §-ban foglaltak szerint.

9. § (1) Az eIDAS rendelet 24. cikk (1) bekezdés *a)* pontja szerinti esetben a regisztráció során a természetes személy tanúsítvány alany személyazonosságát az általa bemutatott személyazonosításra alkalmas hatósági igazolvány alapján az E-ügyintézési tv. 82. § (6) bekezdése szerinti nyilvántartásban ellenőrizni kell.

(2) A regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét a tanúsítvány alany - nem természetes személy esetében képviselője - nyilatkozatban, saját kezű aláírásával ellátva igazolja.

(3) Nem természetes személy tanúsítvány alany esetén a nem természetes személy képviselőjét a bizalmi szolgáltató azonosítja, valamint a képviseleti jogosultságát ellenőrzi.

(4) Ügyintézési célra felhasználható tanúsítvány kizárólag akkor adható ki, valamint aláírás-létrehozó adat kizárólag akkor hozható létre, ha a (2)-(3) bekezdés szerinti ellenőrzés eredményes volt.

(5) A regisztrációt végző szervezet ügyintézője aláírásával igazolja, hogy a hatósági igazolványon szereplő arckép megfeleltethető a természetes személy tanúsítvány alany arcának és az igazolványban szereplő aláírás azonos a (3) bekezdés szerinti nyilatkozatot igazoló aláírásával.

(6) Ha a regisztrációt végző szervezet nem a regisztrációt követően azonnal, ugyanazon a helyszínen adja át az aláírás létrehozásához használt adatot, illetve az aláírást létrehozó eszközt a tanúsítvány alanyának vagy képviselőjének − ideértve, ha az átadást más bizalmi szolgáltató végzi −, az aláírás létrehozásához használt adat vagy aláírást létrehozó eszköz átadását megelőzően az ellenőrzést ismételten el kell végezni.

(7) Az aláírás létrehozásához használt adat és az aláírást létrehozó eszköz meghatalmazással történő átvétele esetén az átvevő meghatalmazottat is a tanúsítvány alannyal megegyező módon ellenőrizni kell, és az ellenőrzés elvégzését alátámasztó iratokat a meghatalmazással együtt meg kell őrizni.

10. § (1) A helyszíni ellenőrzéssel végzett regisztrációt a 9. § szerint, az e §-ban foglalt eltérésekkel kell elvégezni.

(2) A regisztrációt végző szervezet a regisztrációt külső helyszínen is lefolytathatja, ha azonos biztonsági körülmények között biztosítható a tanúsítvány alanyának vagy képviselőjének személyazonosságának ellenőrzése.

(3) Ha a külső helyszíni ellenőrzésnél az E-ügyintézési tv. 82. § (6) bekezdése szerinti központi nyilvántartásban történő ellenőrzés nem biztosítható, a külső helyszíni regisztráció a központi nyilvántartásban történő ellenőrzés nélkül lefolytatható, de a bizalmi szolgáltató a központi nyilvántartásban történő ellenőrzést legkésőbb az aláírást létrehozó eszköz átadásáig köteles lefolytatni.

11. § (1) A feltételes regisztráció során létrehozott tanúsítvány nem érvényes. A feltételes regisztráció során a regisztrációt végző szervezet a 9. és 10. § szerint, az e §-ban foglalt eltérésekkel a személy részére előzetesen elkészíti az elektronikus aláírás létrehozásához használt adatot, illetve az elektronikus aláírást létrehozó eszközt, és azt az e § rendelkezése szerint aktiválja.

(2) A feltételes regisztrációra

a) a személy kérelmére az általa megadott adatokkal, az E-ügyintézési tv. 82. § (6) bekezdése szerinti központi nyilvántartásban történő ellenőrzés elvégzését követően, vagy
b) jogszabály felhatalmazása alapján, állami nyilvántartás adataira alapozva

kerülhet sor.

(3) Az előre elkészített aláírás létrehozásához használt adat és elektronikus aláírást létrehozó eszköz a személy részére átadható

a) a regisztrációs feladatot ellátó szervezetnél,
b) a regisztrációs szervezet külső helyszíni kézbesítésével, vagy
c) postai tértivevényes, hivatalos kézbesítésű küldeményként, saját kézhez történő kézbesítés kikötése esetén.

(4) A tanúsítvány aktiválása a sikeres kézbesítést igazoló irat rendelkezésre állását követően haladéktalanul elvégezhető. A bizalmi szolgáltató a tanúsítvány használatát az aláíró általi előzetes aktiváláshoz kötheti.

(5) Ha a sikeres kézbesítést igazoló okmány 30 napon belül nem érkezik vissza, a tanúsítványt vissza kell vonni.

12. § (1) Távoli elektronikus aláírás esetén az aláírás létrehozásához használt adat és az aláírást létrehozó eszköz átadása alatt a távoli elektronikus aláírás létrehozásához szükséges információ átadását kell érteni.

(2) Ha az aláírás létrehozásához vagy érvényesítéséhez használt adatot a tanúsítvány alany távoli eléréssel töltheti le saját tároló eszközére, az aláírás létrehozásához használt adat és az aláírást létrehozó eszköz átadása alatt a letölthető információhoz való hozzáférést biztosító információ átadását kell érteni.

5. A kiadmányozásra nem jogosult személy (ügyintéző) által használt aláíráshoz tartozó tanúsítvánnyal szembeni követelmények

13. § (1) Az ügyintéző által saját nevében hivatalosan használt elektronikus aláírására - ide nem értve a hatóság nevében tett hivatalos nyilatkozatot (kiadmányozás) - a 7-12. § szerinti követelmények az e §-ban meghatározott eltérésekkel irányadók.

(2) Az ügyintézésben közreműködő személyek elektronikus aláíráshoz szükséges adatokkal, valamint eszközökkel történő ellátásához a regisztráció - ideértve az aláírás létrehozásához szükséges adatok, eszközök átadását, valamint a 9. § (6) bekezdése szerinti ellenőrzést - az ügyintézést biztosító állami szerv személyzeti nyilvántartására alapozva is lefolytatható.

(3) Ha a regisztráció nem az elektronikus ügyintézést biztosító állami szerv személyzeti nyilvántartására alapozva történik, a regisztrációt kezdeményezheti az elektronikus ügyintézést biztosító szerv nevében eljáró, a 9. és 10. § szerint azonosított természetes személy

a) a hitelesítés-szolgáltatóhoz benyújtott igényléssel, amelyet a bizalmi szolgáltatónak az adatok ellenőrzésére feljogosított képviselője előtt ír alá, vagy
b) közokiratba foglalt igényléssel.

(4) A (2) bekezdés szerinti regisztrációt követően a bizalmi szolgáltató köteles az igénylést kiállító hatóságot a tanúsítvány kibocsátásának és az aláírás-létrehozó adat előállításának tényéről írásban értesíteni. Az aláírás-létrehozó adat és a tanúsítvány átvételét az ügyintézést biztosító állami szervnek ugyancsak írásban kell igazolnia. Az átvétel vagy a visszaigazolás elmaradása esetén az ügyintézést biztosító állami szervet az átvételre, illetve annak igazolására ismételten fel kell hívni. Ha a kézbesítés a felhívást követő 30 napon belül nem valósul meg, a tanúsítványt vissza kell vonni.

(5) Az elektronikus ügyintézést biztosító szerv az elektronikus tájékoztatás szabályai szerint közzéteszi

a) az elektronikus aláírási, illetve bélyegzési szabályzatát, mely szabályzatban kell rendelkezni arról, hogy az elektronikus ügyintézést biztosító szerv nevében használt elektronikus aláírás, bélyegző tartalmazza-e az ügyintézést biztosító szerv megnevezését, valamint rögzíti, hogy az aláírás-létrehozó adat előállításához szükséges regisztráció során a hatóság nevében kiadmányozásra való jogosultságot milyen eljárással (dokumentummal) kell a bizalmi szolgáltatónál igazolni,
b) az elektronikus aláírással az ügyfelekkel való kapcsolattartásra feljogosított természetes személyek családi és utónevét, aláírási tanúsítványának nyilvános adatait, az aláírás automatizált ellenőrzéséhez szükséges címet,
c) az időpont megjelölésével és a *b)* pont szerinti adatokkal azt a tényt, ha egy tanúsítvány visszavonásra került vagy egyéb okból már nem alkalmas az ügyintézést biztosító szerv nevében történő eljárásra; az elektronikus bélyegző az erre vonatkozó közlés közzétételi időpontjától a szervezet nevében további dokumentumhitelesítésre nem alkalmas.

(6) Ha a bizalmi szolgáltató a tanúsítványt

a) visszavonta, az aláírás vagy bélyegző a visszavonás időpontjától,
b) felfüggesztette, az aláírás vagy bélyegző a felfüggesztés időtartama alatt

dokumentumhitelesítésre nem alkalmas.

(7) Az (5) bekezdés *b)* és *c)* pontja szerinti információkat a tanúsítvány érvényességének lejártától számított 10 évig kell a honlapon hozzáférhetővé tenni.

(8) Az e § és a 6. alcím szerinti tanúsítvány tekintetében a (2) bekezdés szerinti regisztrációt a személyes megjelenéssel egyenértékűnek kell tekinteni.

6. A kiadmányozásra feljogosított személy (ügyintéző) által használt aláíráshoz tartozó tanúsítvánnyal szembeni követelmények

14. § (1) Az elektronikus ügyintézést biztosító szerv nevében kiadmányozásra feljogosított természetes személy által e feladatkörében is használt aláírás esetén a 13. § szerinti szabályoknak megfelelő aláírások az e §-ban meghatározott eltérésekkel használhatóak.

(2) Kiadmányozásra feljogosított személy e minőségében olyan elektronikus aláírást használhat, amelynél a hozzá tartozó hitelesítési rend szerepel az E-ügyintézési tv. szerinti bizalmi felügyelet által vezetett nyilvántartásban.

(3) Jogszabályban meghatározott védelem alá eső tisztséget, valamint nemzetbiztonsági ellenőrzés alá eső jogviszonyt betöltő személyek az 5. § szerinti ügyekben csak a 3. § (1) bekezdése szerint hitelesített kulcsokat alkalmazó elektronikus aláírást használhatnak.

(4) Az (1) bekezdés szerinti feladatra alkalmas tanúsítványt és aláírás-létrehozó adatot jogszabályban meghatározott védelem alá eső tisztséget, valamint nemzetbiztonsági ellenőrzés alá eső jogviszonyt betöltő személyek csak a kormányzati hitelesítés-szolgáltatás keretében vehetnek igénybe.

(5) Az elektronikus ügyintézést biztosító szerv a tájékoztatási kötelezettségének teljesítésekor a 13. § (5) bekezdés *b)* pontja szerinti adatokon túl külön közzéteszi az adott személynek az ügyintézést biztosító szerv nevében elektronikus aláírással történő kiadmányozásra való jogosultságát.

(6) Az (5) bekezdés, valamint a 13. § (5) bekezdés *c)* pontja szerinti információkat a tanúsítvány visszavonásától vagy érvényességének lejártától számított 10 évig kell a honlapon hozzáférhetővé tenni.

7. Az ügyintézési célú elektronikus bélyegző létrehozásához használt tanúsítvánnyal szembeni követelmények

15. § (1) Az elektronikus ügyintézést biztosító szerv számára kibocsátott ügyintézési célú elektronikus bélyegző tanúsítványához szükséges regisztrációt a 13. § (3) bekezdése szerinti személy kezdeményezheti.

(2) A regisztrációhoz meg kell adni a regisztrációt kérő ügyintézést biztosító állami szerv, valamint az ügyintézési célú elektronikus bélyegzőhöz rendelt eszköz egyértelmű azonosításához szükséges, a tanúsítványban szerepeltetendő adatokat és az ügyintézést biztosító állami szervnél a kapcsolattartásért felelős személy elérési adatait.

(3) Az (1) bekezdés szerinti regisztrációt követően a bizalmi szolgáltató köteles az igénylést kiállító elektronikus ügyintézést biztosító szervet a tanúsítvány kibocsátásának és a bélyegző tanúsítványában szereplő, a bélyegzés létrehozásához felhasznált adat előállításának tényéről írásban értesíteni. A bélyegző létrehozásához használt adat és a tanúsítvány átvételét az elektronikus ügyintézést biztosító szervnek ugyancsak írásban kell igazolnia. Az átvétel vagy a visszaigazolás elmaradása esetén az elektronikus ügyintézést biztosító szervet az átvételre, illetve annak igazolására ismételten fel kell hívni. Ennek eredménytelensége esetén a tanúsítványt vissza kell vonni.

16. § Az elektronikus ügyintézést biztosító szerv az általa ügyintézés során használt elektronikus bélyegző és a képviselője által használt elektronikus aláírás létrehozásához használt adatra vonatkozó iratokat, a hozzájuk kapcsolt tanúsítványokat, az elektronikus aláírási és bélyegzési szabályzatokat a maradandó értékű köziratokra vonatkozó szabályok szerint megőrzi, és a megőrzési idő letelte után az illetékes levéltárnak átadja.

19. § (1) Ez a rendelet a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendelet III. fejezetének végrehajtásához szükséges rendelkezéseket állapít meg.

84/2012. (IV. 21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről

http://njt.hu/cgi_bin/njt_doc.cgi?docid=148204.342121

4. A Kormány által kötelezően biztosított szabályozott elektronikus ügyintézési szolgáltatások és a központi elektronikus ügyintézési szolgáltatások szolgáltatói

4. § A Kormány a szabályozott elektronikus ügyintézési szolgáltatások, illetve a központi elektronikus ügyintézési szolgáltatások szolgáltatóiként az alábbi szervezeteket jelöli ki:

a) az ügyfél elektronikus ügyintézési cselekményekről történő időszaki értesítése vonatkozásában a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

b) a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény szerinti összerendelési nyilvántartás szolgáltatás vonatkozásában az e-közigazgatásért felelős minisztert, aki e feladatának ellátásához az IdomSoft Zrt. közreműködését igénybe veheti,

c) a biztonságos kézbesítési szolgáltatás vonatkozásában a Magyar Posta Zrt.-t, valamint a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

d) az űrlapbenyújtás támogatási szolgáltatás esetében

da) az ÁNYK űrlapbenyújtás támogatási szolgáltatás vonatkozásában a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

db) az elektronikus űrlapkitöltés-támogatási szolgáltatás tekintetében a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

e) az elektronikus dokumentumtárolási szolgáltatás vonatkozásában a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

*f)*a Kormány által kötelezően biztosított elektronikus azonosítási szolgáltatás természetes személy ügyfelek részére történő szolgáltatás vonatkozásában a NISZ Nemzeti InfokommunikációsSzolgáltatóZrt.-t,

g) a kormányzati hitelesítés-szolgáltatás vonatkozásában

ga) a nemzetbiztonsági szolgálatok, a Terrorelhárítási Központ, valamint a Rendőrség tanúvédelemmel foglalkozó munkatársai tekintetében az irányító minisztert, a tanúsítvány-igénylő regisztrációjával kapcsolatos feladatok tekintetében az érintett nemzetbiztonsági szolgálat, a Terrorelhárítási Központ, illetve a Rendőrség közreműködésével,

*gb)*egyéb esetekben a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t, a tanúsítvány-igénylő regisztrációjával kapcsolatos feladatok tekintetében a közigazgatási szervek személyügyi szervezeti egységeinek közreműködésével,

h) a központi dokumentumhitelesítési ügynök szolgáltatás tekintetében a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

i) az azonosításra visszavezetett dokumentumhitelesítés szolgáltatás vonatkozásában a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

j) az iratérvényességi nyilvántartás vonatkozásában a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt-t,

k) a kormányzati elektronikus aláírás ellenőrzési szolgáltatás vonatkozásában a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

l) a központi azonosítási ügynök szolgáltatás vonatkozásában a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

m) az általános célú elektronikus kéreleműrlap szolgáltatás vonatkozásában a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,

n) a papíralapú irat átalakítása hiteles elektronikus irattá, valamint az elektronikus irat hiteles papír alapú irattá alakítása szolgáltatás vonatkozásában a Magyar Posta Zrt.-t,

o) a központi kormányzati szolgáltatás busz szolgáltatás vonatkozásában az IdomSoft Zrt.-t,
q) a személyre szabott ügyintézési felület szolgáltatás tekintetében a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,
r) az iratkezelő rendszerek közötti iratáthelyezés szolgáltatás tekintetében a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,
s) a központi érkeztetési ügynök szolgáltatás tekintetében a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t,
t) a központi kézbesítési ügynök szolgáltatás tekintetében a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t.

4/A. § A 4. § *c)* pontja szerinti biztonságos kézbesítési szolgáltatásához kapcsolódóan a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. kézbesítési tárhelyet biztosít

a) természetes személyek részére (Központi Ügyfél-regisztrációs Nyilvántartás regisztrációhoz kapcsolódó tárhely),
b) gazdálkodó szervezetek részére (gazdálkodó szervezetek számára biztosított tárhely), valamint
c) közfeladatot ellátó szervek részére (hivatali tárhely).

5. § A Kormány az elektronikus fizetési és elszámolási rendszer szolgáltatójaként a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t jelöli ki.

6. § (1) A kijelölt szolgáltatók olyan szabályozott vagy központi elektronikus ügyintézési szolgáltatás ellátásába is bevonhatják - erre vonatkozó megállapodás, és a szükséges pénzügyi forrás biztosítása esetén - a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t és a Magyar Posta Zrt.-t, amely szolgáltatásoknál a 4. §-ban ez nincs kifejezetten előírva.

(2) A NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. és a Magyar Posta Zrt. az e rendelet szerinti tevékenységeinek ellátására közszolgáltatási szerződést köt az e-közigazgatásért felelős miniszterrel.

(3) Az egységes kormányzati ügyiratkezelő rendszerhez kapcsolódóan megvalósuló papíralapú irat hiteles elektronikus irattá történő átalakítására vonatkozóan a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. szerződést köt a Magyar Posta Zrt.-vel.

5. Kormány által kötelezően nyújtandó azonosítási szolgáltatások regisztrációja

7. § (1) A Központi Ügyfél-regisztrációs Nyilvántartás regisztrációs szerveként a Kormány a fővárosi és megyei kormányhivatalokat, a fővárosi és megyei kormányhivatalok járási (fővárosi kerületi) hivatalait, az e-közigazgatásért felelős minisztert, a Nemzeti Adó- és Vámhivatalt, a Magyar Posta Zrt.-t, valamint Magyarország diplomáciai és konzuli képviseleteit jelöli ki. A Kormány Központi Ügyfél-regisztrációs Nyilvántartást vezető szervként az e-közigazgatásért felelős minisztert jelöli ki, aki az adatkezelői feladatok ellátása érdekében adatfeldolgozói szerződést köthet.

2012. évi CLIX. törvény a postai szolgáltatásokról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=155642.338719

4. § Nem postai szolgáltatás

c) fizikai formában meg nem jelenő üzenet (közlés, adat, információ) elektronikus úton történő továbbítása a küldésétől a fogadásig;

33. Személyes adatok védelme, titokvédelmi kötelezettség

54. § (1) A postai szolgáltató a postai szolgáltatás teljesítésével kapcsolatos vagy a szolgáltatás teljesítése során tudomására jutott adatokat - az 55. § (1)-(5) bekezdésében foglalt eltérésekkel, közérdeken alapuló célból, az információs önrendelkezési jogról és az információszabadságról szóló törvényben foglaltak figyelembevételével - e törvény felhatalmazása alapján - adatkezelőként eljárva használhatja fel és továbbíthatja.

(2) Az (1) bekezdés szerinti adatkezelés

a) célja: a postai szolgáltatási szerződés teljesítése, a teljesítés elszámolása, igazolása és utólagos ellenőrzése, a Hatóság részére történő adatszolgáltatás, továbbá e törvényben meghatározott egyéb cél;

b) időtartama: e törvény vagy a felhasználó eltérő rendelkezése hiányában a postai küldemény feladását követő naptári év vége.

(3) A postai szolgáltatás teljesítése nem tehető függővé olyan személyes vagy más adat megadásától, vagy olyan célú adatkezeléshez való hozzájáruló nyilatkozat megtételétől, amely a postai szolgáltatás feladó által igényelt tartalmú elvégzéséhez nem szükséges.

(4) A postai szolgáltató a postai szolgáltatás teljesítésével kapcsolatos, valamint a szolgáltatás teljesítése során tudomására jutott adatokat kizárólag a postai szolgáltatási szerződés teljesítése, a teljesítés igazolása, elszámolása és utólagos ellenőrzése céljából továbbíthatja harmadik országban lévő adatkezelő vagy adatfeldolgozó részére.

(5) Az egyetemes postai szolgáltató, a közvetlen vagy közvetett tulajdonában álló gazdasági társaság és a velük szoros kapcsolatban álló vállalkozás a törvény vagy az érintett hozzájárulása alapján kezelt, közösen használt informatikai rendszerben nyilvántartott, valamely természetes személy ügyfél azonosítására szolgáló adatot az információs önrendelkezési jogról és az információszabadságról szóló törvény rendelkezései alapján helyesbíti, ha tudomására jut, hogy az adat nem felel meg a valóságnak. Nem felel meg a valóságnak az adat különösen akkor, ha az adat megváltozásának tényét vagy az adat helytelenségét és a valóságnak megfelelő adatot okirattal vagy személyes nyilatkozattal igazolták.

(6) Az (5) bekezdést a nem természetes személy ügyfélről az egyetemes postai szolgáltató, a közvetlen vagy közvetett tulajdonában álló gazdasági társaság és a velük szoros kapcsolatban álló vállalkozás által kezelt adatokra is alkalmazni kell.

55. § (1) A postai szolgáltató az általa kezelt postai küldemény tartalmát csak a szolgáltatás teljesítéséhez szükséges mértékben ismerheti meg.

(2) A postai szolgáltató a postai szolgáltatása keretében

a) a zárt postai küldeményt - a (4) bekezdésben foglaltak kivételével - nem bonthatja fel;
b) a nem zárt postai küldeményeket csak a felvételhez, gyűjtéshez, feldolgozáshoz, szállításhoz, kézbesítéshez szükséges adatok megállapítása érdekében és annak megfelelő mértékben tanulmányozhatja;
c) a szolgáltatás teljesítése során tudomására jutott adatot - a feladó, a címzett (illetve az egyéb jogosult átvevő), valamint a (6) bekezdésben említett szervezetek kivételével - mással nem közölhet;
d) a postai küldeményt - tartalmának megismerése céljából - a feladó, a címzett (illetve az egyéb jogosult átvevő), valamint a (6) bekezdésben említett szervezetek kivételével másnak át nem adhatja;
e) a szolgáltatás teljesítéséről - a feladó, a címzett (illetve az egyéb jogosult átvevő), valamint a (6) bekezdésben említett szervezetek kivételével - másnak tájékoztatást nem adhat.

(3) A (2) bekezdés *d)* pontja alkalmazásában a feladóval megegyező jogosultsággal rendelkezőnek kell tekinteni azt a személyt, aki a postai küldemény feladását igazoló dokumentumot bemutatja. A (2) bekezdés *c)* és *e)* pontja tekintetében a feladóval megegyező jogosultsággal rendelkezőnek kell tekinteni azt a személyt is, aki a postai küldemény egyedi azonosító adatát (például kód, küldeményazonosító), továbbá szükség esetén a feladó és címzett nevét és a küldemény címét a postai szolgáltatóval elektronikus hírközlési úton (távközlő berendezés, internet) közli.

(4) A postai szolgáltató a zárt postai küldeményt felbonthatja, ha

a) a küldemény burkolata oly mértékben sérült, hogy tartalmának megóvása érdekében a felbontása indokolt, és felbontás nélküli átcsomagolással a küldemény tartalmának a megóvása nem biztosítható;
b) a küldemény tartalma által okozott veszély elhárítása érdekében ez indokolt;
c) a 42. § (6) bekezdés *b)* és *c)* pontjában meghatározott eset áll fenn.

(5) A postai küldemény felbontását a 42. § (8) bekezdése szerint kell elvégezni, azzal, hogy a felbontás tényét a küldeményre rá kell vezetni, továbbá, ha erre lehetőség van, a felbontásról, a felbontás okáról a feladót értesíteni kell.

(6) A postai szolgáltatónak és a postai közreműködői tevékenységet végző személynek vagy szervezetnek megfelelő szervezési és műszaki intézkedésekkel biztosítania kell a postai szolgáltatás teljesítése során kezelt küldemények, szöveges közlemények vagy közlések

titkosságát. A postai szolgáltató és a postai közreműködői tevékenységet végző személy vagy szervezet - a jogszabályi feltételek fennállása és erre irányuló megkeresés esetén - köteles a postai küldeményt, szöveges közleményt vagy közlést átadni vagy bemutatni az annak megismerésére külön törvényben feljogosított szervezeteknek, továbbá azok megfigyelését, tárolását vagy a küldeménybe, szöveges közleménybe más módon történő beavatkozást lehetővé tenni.

(7) A postai szolgáltató a postai szolgáltatáshoz kapcsolódó valamennyi okiratot a kiállítástól vagy az okirat érvényességi idejének lejáratától számított egy évig köteles őrizni.

47. Vegyes rendelkezések

75. § (1) A Kormány által a papír alapú irat hiteles elektronikus irattá alakítása, valamint az elektronikus irat hiteles papír alapú irattá alakítása szolgáltatás nyújtására rendeletben kijelölt postai szolgáltató jogosult olyan nem postai szolgáltatás nyújtására, melynek keretében vállalja a címzett részére kézbesítendő postai küldemény felbontását, arról elektronikus másolat készítését, és címzetthez eljuttatását a címzett rendelkezései szerint. A kijelölt szolgáltató ennek keretében jogosult hiteles elektronikus másolat készítésére is a papír alapú irat hiteles elektronikus irattá alakítására irányuló szolgáltatás szabályai szerint azzal, hogy az így készített elektronikus másolat bizonyító ereje megegyezik az eredeti papír alapú irat bizonyító erejével.

(2) Az (1) bekezdésben meghatározott postai szolgáltató jogosult olyan nem postai szolgáltatás nyújtására, melynek keretében a postai feladás részeként a feladó által átadott elektronikus dokumentumról papír alapú másolatot készít, majd azt kézbesíti. A Kormány által rendeletben kijelölt postai szolgáltató ennek keretében jogosult hiteles papír alapú másolat készítésére is az elektronikus irat hiteles papír alapú irattá alakítására irányuló szolgáltatás szabályai szerint azzal, hogy az így készített papír alapú másolat bizonyító ereje megegyezik az eredeti elektronikus irat bizonyító erejével.

335/2012. (XII. 4.) Korm. rendelet a postai szolgáltatások nyújtásának és a hivatalos iratokkal kapcsolatos postai szolgáltatás részletes szabályairól, valamint a postai szolgáltatók általános szerződési feltételeiről és a postai szolgáltatásból kizárt vagy feltételesen szállítható küldeményekről

http://njt.hu/cgi_bin/njt_doc.cgi?docid=156666.347726

1/A. § (1) Postai szolgáltatási szerződés leplezésének minősül a jogviszony különösen akkor, ha bármely szervezet a saját gazdasági vagy egyéb tevékenységével összefüggő tartalmú küldeményét olyan - vele munkavégzésre irányuló, illetve tagsági jogviszonyban álló - természetes személlyel juttatja el a címre, aki más szervezettel már ilyen vagy bármely más

munkavégzésre irányuló jogviszonyban áll, és ennek alapján tevékenysége részben vagy egészben küldemények rendeltetése szerinti helyre történő eljuttatására irányul.

(2) A postai szolgáltatásra a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól szóló rendeletben foglaltakat nem kell alkalmazni, amennyiben a postai szolgáltató internetes honlapján közzétett és minden postai szolgáltatóhelyen a felhasználók által megtekinthető általános szerződési feltételei megfelelnek a 2. §-ban foglalt követelményeknek és a postai szolgáltatási szerződés ezen általános szerződési feltételek alapján jött létre.

2. § A postai szolgáltatók általános szerződési feltételeinek kötelező tartalmi elemei:

a) a postai szolgáltatás vagy a postai szolgáltatáshoz kapcsolódó többletszolgáltatás megnevezése;
b) a postai szolgáltatás keretében feladható vagy kézbesíthető küldemények méret- és tömeghatárai;
c) a feltételesen vagy különleges előírások figyelembevételével szállított tartalmakkal kapcsolatos szabályok;
d) külföldre szóló postai küldemény esetében a cím szerinti és a kezelésben részt vevő országban hatályos behozatali tilalommal (korlátozással) kapcsolatos szabályok;
e) a cím adattartalmával és annak feltüntetésével kapcsolatos szabályok;
f) a szolgáltatás minősége;
g) a szolgáltatás díjának megfizetési módjai;
h) a kézbesítés feltételeivel kapcsolatos felhasználói jogok és kötelezettségek;
i) a szolgáltatással kapcsolatos panaszok és a panaszkezelés felhasználókat érintő szabályai;
j) a szolgáltató adatkezelésének felhasználókat érintő szabályai;
k) a szolgáltatással kapcsolatos felelősségi szabályok, a kártérítési igény érvényesítésével kapcsolatos jogok és kötelezettségek, valamint az igényérvényesítés módjának meghatározása;
l) a postai szolgáltatásokról szóló 2012. évi CLIX. törvény (a továbbiakban: Postatv.) vagy e rendelet alapján az általános szerződési feltételekben megjelenítendő, a postai szolgáltatás nyújtásának és igénybevételének egyéb részletes feltételei.

2. A postai küldemények felvétele

4. § (1) Az egyetemes postai szolgáltatás keretében feladott küldemények esetében megfelelőnek kell tekinteni a postai küldemény címzését, amennyiben az az alábbi sorrendben, latin betűkkel, arab számokkal (szükség esetén római számmal) a következő adatokat tartalmazza:

a) a címzett (címzettek) neve, elnevezése;
b) a küldemény rendeltetési helye (a település neve);
c) közterületi cím (út, utca, egyéb közterület neve és a házszám), és ha van a közelebbi címadatokként a lépcsőház-, emelet-, ajtószám, ezek hiányában helyiség megjelölése,

(a közterületi cím és a közelebbi címadatok a továbbiakban együtt: címhely);

d) a címhely irányítószáma.

(2) Az egyetemes postai szolgáltatás keretében külföldre címzett küldemények esetében fel kell tüntetni a rendeltetési ország nevét is.

(3) Az egyetemes postai szolgáltatás keretében feladható küldemények címzésében szereplő adatok elhelyezésének módját és a címzés egyéb tartalmi és formai követelményeit az egyetemes szolgáltató az általános szerződési feltételeiben határozza meg.

5. § Az egyetemes postai szolgáltatások keretében küldeményenkénti díjszabás szerint feladott küldeményekkel kapcsolatos postai szolgáltatás igénybevételéhez szükséges nyomtatványokat - a feladáshoz szükséges mennyiségben - a szolgáltató díjmentesen bocsátja rendelkezésre. E nyomtatványokat a postai szolgáltató által kitöltendő adatok kivételével hiánytalanul, kitöltötten kell a küldemény feladásakor a szolgáltató számára átadni.

7. § (1) A postai szolgáltató a könyvelt küldeményre vonatkozó postai szolgáltatási szerződés létrejöttének igazolásául köteles a feladó részére a feladást igazoló okiratot átadni. Az okiratnak tartalmaznia kell legalább

a) a postai szolgáltató nevét és a felvétel napját, időgarantált szolgáltatás esetében az időpontját is;
b) a feladó nevét és címét;
c) a küldemény egyedi azonosító jelzését;
d) a postai szolgáltató által az okirat hitelesítésére alkalmazott jelzést;
e) küldeményenkénti díjszabás szerint feladott küldemény esetében a címzésében szereplő adatokat;
f) az általános szerződési feltételek elérhetőségéről szóló tájékoztatást.

(2) A feladást igazoló okiraton tájékoztatást kell adni arról, hogy a szerződésre a Postatv. és e rendelet rendelkezései az irányadók.

(3) A postai szolgáltató és a feladó egyedi szerződésben az (1) és a (2) bekezdésben foglaltaktól eltérő tartalmú feladást igazoló okirat alkalmazásában is megállapodhatnak, továbbá megállapodhatnak abban is, hogy a feladást igazoló okiratot mindkét szerződő fél által elektronikusan is visszakereshető, jelzés vagy elektronikus formában rögzített adatbázis is helyettesítheti.

(4) A feladónak a könyvelt postai küldeményen, annak csomagolásán vagy az ahhoz tartozó listán - kivéve, ha jelzése alapján a küldemény pályázatot vagy versenytárgyalási ajánlatot tartalmaz - fel kell tüntetnie az (1) bekezdés *b)* pontjában meghatározott adatokat, amelyeket a postai szolgáltató a küldemény esetleges visszakézbesítése során köteles figyelembe venni.

8. § A postai szolgáltató a postai küldemények feladását igazoló okiratot, valamint a postai küldeményt és annak kísérő okiratát közcélú vagy postai szolgáltatásra vonatkozó tájékoztatást

tartalmazó reklám lenyomattal is elláthatja, amennyiben az a feladási és címadatok áttekinthetőségét nem zavarja.

3. A postai küldemény kézbesítésének általános szabályai

9. § (1) A postai küldeményt a címzett vagy e rendelet eltérő rendelkezésének hiányában az egyéb jogosult átvevő részére kell kézbesíteni. Egyéb jogosult átvevőnek a 15. § (4) bekezdése és a 16. § (4) bekezdése szerinti alkalmi átvevő, a 16. § (3) bekezdésében meghatározott helyettes átvevő, a 19. §-ban meghatározott meghatalmazott, valamint a 20. §-ban meghatározott közvetett kézbesítő minősül.

(2) A postai küldeményt - a (3)-(6) bekezdésben, valamint a 12. § (4a) bekezdésében foglalt kivételekkel - a küldemény címén kell kézbesíteni. A küldemény címe az a cím, amelyet a feladó feltüntetett a küldeményen, annak csomagolásán vagy ahhoz tartozó listán.

(3) A postai küldeményt a címében feltüntetettől eltérően azon a helyen kell kézbesíteni,

a) amelyet a feladó vagy a címzett - ha a postai szolgáltatási szerződés tartalmazta a feladó vagy a címzett részére a címváltoztatás lehetőségét, és a felhasználó élt is ezzel - a legkésőbb adott meg,

b) amelyet a címzett a postai szolgáltatóval kötött, olyan tartalmú szerződésben adott meg, mely a részére érkező küldemény kézbesítését a címtől eltérő helyen biztosítja.

(4) A postai szolgáltató a települések belterületén kívüli lakott helyekre címzett levélszekrénybe kézbesíthető küldemények kézbesítését, valamint - a kézbesítés megkísérlésének mellőzésével - a személyes átadással kézbesítendő küldemény érkezéséről szóló értesítő elhelyezését a közutak mentén a postai szolgáltató által kijelölt helyen, a címhelyekhez rendelten telepített és üzemeltetett kézbesítésre alkalmas eszköz útján biztosíthatja.

(5) Ha személyes kézbesítést igénylő küldemény esetében a címzett vagy egyéb jogosult átvevő a kézbesítés megkísérlésekor nem tartózkodik a címen, a postai szolgáltató - értesítő hátrahagyása mellett - kézbesítési ponton való kézbesítéssel, vagy a 25. § (1) bekezdés *a), b), e), f)* és *g)* pontjában meghatározott esetekben a feladó részére történő visszakézbesítéssel teljesítheti a postai szolgáltatási szerződést.

10. § (1) A postai szolgáltató az általános szerződési feltételeiben meghatározott címadatokon kívül a postai küldeményre feljegyzett egyéb adatokat nem köteles figyelembe venni.

(2) A postai szolgáltató nem köteles vizsgálni, hogy a címhelyen van-e más ugyanolyan nevű természetes személy, aki a küldeményre igényt tarthat.

(3) A jogi személy és egyéb szervezet (a továbbiakban együtt: szervezet) számára címzett küldeménynek tekinthető a küldemény akkor is, ha a címzésben a szervezet neve vagy címe mellett valamely természetes személy neve is fel van tüntetve.

(4) Ha a címzésben több természetes személy neve szerepel, a postai küldemény a megnevezettek bármelyikének kézbesíthető.

9. Az átvételi jogosultság és a személyazonosság igazolása

21. § (1) A címhelyen történő kézbesítéskor - közvetett kézbesítés kivételével - az átvételi jogosultság jogcíméről tett szóbeli nyilatkozattal a jogcím igazoltnak tekintendő. Amennyiben a szóbeli nyilatkozat alapján az átvételi jogosultság jogcíme kétséges, a postai szolgáltató kérheti a jogcím fennállásának további igazolását. A közvetett kézbesítő az átvételi jogosultság jogcímének fennállását a 20. § (10) bekezdése szerinti névre szóló igazolással igazolja.

(3) A hivatalos iratnak nem minősülő könyvelt küldemény címhelyen történő kézbesítése esetén az igazolt jogcímmel rendelkező átvevő személyazonosságának igazolására alkalmas okmány elnevezését, betűjelét és számát - az alkalmi átvevőnek történő kézbesítés kivételével - a postai szolgáltató nem köteles rögzíteni. Meghatalmazottnak történő kézbesítés esetében a személyazonosság igazolására csak az a hatósági igazolvány alkalmas, amelyben a meghatalmazott nevén kívül legalább egy olyan - a személyazonosság megállapítására alkalmas - adat szerepel, amelyet a meghatalmazás is tartalmaz.

22. § (1) Természetes személy címzett részére küldött postai küldeménynek kézbesítési ponton történő kézbesítésekor az átvételi jogosultság jogcímének fennállása vonatkozásában a küldemény átvétele érdekében megjelenő személy szóbeli nyilatkozata irányadónak tekinthető, amennyiben bemutatja, illetve a postai szolgáltató kérésére átadja a küldemény érkezéséről szóló értesítőt. Helyettes átvevő esetében a lakcímének vagy tartózkodási címének a postai küldemény címével vagy az utánküldési címmel való egyezőségét is igazolni kell. A postai szolgáltató jogosult a kézbesítést megelőzően az átvételi jogosultság jogcímének további igazolását kérni.

(2) A szervezet mint címzett esetében a vezető átvételi jogosultságát olyan eredeti okirattal vagy arról készített közokiratba foglalt vagy egyszerű másolattal igazolhatja,

a) amely egy évnél nem régebbi és a szervezetre vonatkozó jogszabály alapján egyébként alkalmas a vezetői minőség igazolására, vagy

b) amelyet a postai szolgáltató az *a)* pontban foglaltakon túl az általános szerződési feltételei szerint e célból

elfogad.

(2a) A postai szolgáltató a bemutatott okiratok közül a később kiállítottat tekinti irányadónak, a (2) bekezdés *a)* pontja szerinti esetben az okiratok érvényességét, hatályosságát csak az egy évnél nem régebbi keltezés tekintetében vizsgálja. A postai szolgáltató felkérheti a vezetői minőségét igazolni kívánó személyt a bemutatott okirat elfogadandóságának jogszabályi alátámasztására, melynek elmaradása esetén a vezetői minőséget nem köteles igazoltnak tekinteni.

(3) A könyvelt küldemény kézbesítési ponton történő kézbesítésekor az igazolt jogcímmel rendelkező átvevő a személyazonosságát az arra alkalmas hatósági igazolvány postai szolgáltató

részére történő bemutatásával igazolja. Meghatalmazottnak történő kézbesítés esetében a személyazonosság igazolására csak az a hatósági igazolvány alkalmas, amelyben a meghatalmazott nevén kívül legalább egy olyan - a személyazonosság megállapítására alkalmas - adat szerepel, amelyet a meghatalmazás is tartalmaz.

(4) A kézbesítési ponton történő kézbesítés esetében, amennyiben a küldemény átvétele érdekében megjelenő személy nem mutatja be, illetve a postai szolgáltató kérésére nem adja át a küldemény érkezéséről szóló értesítőt, a küldemény csak az átvételi jogosultság jogcímének és a személyazonosságnak hatósági igazolvánnyal, illetve közhitelű dokumentummal történő igazolását követően kézbesíthető. Helyettes átvevő esetében a lakcímének vagy tartózkodási címének a postai küldemény címével vagy az utánküldési címmel való egyezőségét is igazolni kell.

(5) Könyvelt küldemény kézbesítése esetén a küldemény átadásának igazolásaként a kézbesítési okiraton, vagy az aláírást rögzítő egyéb technikai eszközön

a) címhelyen történő kézbesítés esetén az átvétel jogcímének - kivéve, ha a küldeményt a címzett veszi át - feltüntetése, és a címzett vagy egyéb jogosult átvevő saját kezű aláírása,

b) kézbesítési ponton történő kézbesítés esetén az *a)* pontban foglaltakon túl a címzett vagy egyéb jogosult átvevő személyazonosságát igazoló okmány elnevezésének, betűjelének és számának feltüntetése

szükséges.

(5a) Saját kezű aláírásnak minősül az is, ha a címzett vagy egyéb jogosult átvevő a kézbesítési okiraton vagy a tértivevényen a személyét hitelesen, utólag általa nem vitatható módon tanúsító jelzést helyez el. A jelzés használatának részletes szabályait a postai szolgáltató általános szerződési feltételeiben határozza meg. A jelzés hitelességét tanúsító okiratot a címzett vagy egyéb jogosult átvevő és a postai szolgáltató a jelzés utolsó használatát követő három évig köteles megőrizni.

23. § A postai szolgáltató általános szerződési feltételeiben jogosult a könyvelt küldemény kézbesítését - a 22. §-ban megállapított rendelkezésekben foglaltakon túl - további, az átvételi jogcím és a személyazonosság igazolása vonatkozásában a címzett vagy egyéb jogosult átvevő által kötelezően teljesítendő előírások teljesítésétől függővé tenni.

10. A postai küldemény átvételének megtagadása

24. § (1) A postai küldemény átvétele megtagadásának a címzett vagy a meghatalmazott azonnali átvételtől elzárkózó egyértelmű nyilatkozata minősül. Szervezet esetében a címzett általi megtagadásnak minősül, ha a 15. § (2)-(3) bekezdésében meghatározott személy tagadja meg az átvételt.

(2) Az átvétel megtagadása esetén ennek tényét mint kézbesíthetetlenségi okot a kézbesítési okiraton vagy az aláírást rögzítő egyéb technikai eszközön, valamint a küldeményen vagy a

kísérőokiraton fel kell tüntetni, és a postai küldeményt - értesítő hátrahagyása és rendelkezésre tartási idő biztosítása nélkül - a feladó részére vissza kell kézbesíteni.

(3) Nem minősül a küldemény átvétele megtagadásának, amennyiben

a) a címzett vagy meghatalmazott a kézbesítéskor esedékes díj megfizetését az összeg mértéke vagy a fizetési mód miatt csak a kézbesítési kísérletet követően, a Postatv. 42. § (1) bekezdésében rögzített rendelkezésre tartási időn belül vállalja teljesíteni, vagy

b) a címzetten és meghatalmazotton kívüli egyéb jogosult átvevő nem kívánja átvenni a küldeményt, vagy elzárkózik a kézbesítéskor esedékes díj megfizetésétől, az átvétel jogcímének vagy személyazonosságának igazolásától, továbbá a kézbesítési okirat vagy tértivevény aláírásától vagy az átvétel során feltüntetendő adatok rögzítésétől.

Ezen esetekben a címzett részére a küldemény érkezéséről értesítőt kell hátrahagyni.

11. A postai küldemény kézbesíthetetlensége és a kézbesíthetetlenségi ok jelzése

25. § (1) A postai szolgáltatón kívül álló okból kézbesíthetetlen a postai küldemény a címzett részére, ha

a) a küldemény címzése vagy címe nem megfelelő, vagy a cím nem létező, továbbá ha a címhely azonosításra nem alkalmas, vagy az nem egyértelmű (jelzése: cím nem azonosítható),

b) a címzett a címen nem egyértelműen azonosítható, vagy - különösen a 26. § (3) bekezdése szerint tett bejelentés alapján - nem ismert (jelzése: címzett ismeretlen),

c) a címzett vagy egyéb jogosult átvevő a kézbesítésről szóló értesítésben megjelölt határidő lejártáig a rendelkezésére tartott küldeményért nem jelentkezett (jelzése: nem kereste),

d) a 24. § (1) bekezdése szerinti kézbesíthetetlenségi ok áll fenn (jelzése: átvételt megtagadta),

e) a címzett - a 26. § (3) bekezdése szerinti bejelentés tartalma alapján - elköltözött (jelzés: elköltözött),

f) a levélszekrénybe történő elhelyezéssel vagy személyes átadással történő kézbesítés vagy az értesítő hátrahagyása nem lehetséges (jelzése: kézbesítés akadályozott),

g) a 26. § (3) bekezdése szerinti bejelentés vagy nyilatkozat alapján a természetes személy meghalt, a szervezet megszűnt (jelzése: bejelentve: meghalt/megszűnt).

(2) A kézbesíthetetlenség (1) bekezdésben meghatározott okát a postai szolgáltató az ott meghatározott jelzésnek megfelelően köteles a kézbesítési okiraton vagy az aláírást rögzítő egyéb technikai eszközön, valamint a küldeményen vagy a kísérőokiraton feltüntetni, valamint a postai küldeményt a feladónak visszakézbesíteni.

(3) A postai szolgáltató a kézbesíthetetlenség (1) bekezdésben meghatározott okain belül az általános szerződési feltételeiben megállapítottak szerint további kézbesíthetetlenségi okokat is visszajelezhet a feladó részére.

(4) A postai szolgáltató a kézbesíthetetlenség (1) és (3) bekezdésben meghatározott okáról e-mail, rövid szöveges üzenet vagy egyéb technikai eszköz alkalmazásával tájékoztatja a feladót, ha erről vele egyedi szerződésben vagy az általános szerződési feltételek alapján megállapodott.

12. A postai küldemény kézbesítésének egyéb szabályai

26. § (1) Az írni nem tudó, a latin betűket nem ismerő vagy egyéb ok miatt írásában gátolt címzettnek, vagy egyéb jogosult átvevőnek a könyvelt küldeményt írni tudó, nagykorú tanú jelenlétében kell kézbesíteni. A kézbesítő a kézbesítés előtt a címzett, vagy egyéb jogosult átvevő, továbbá a tanú személyazonosságát a 21. § és 22. § szerint ellenőrzi. A tanú - e minőségének feltüntetése mellett - a kézbesítési okiraton vagy az aláírást rögzítő egyéb technikai eszközön saját nevét írja alá.

(2) A cselekvőképtelen vagy a cselekvőképességet kizáró gondnokság alatt álló természetes személy részére címzett személyes kézbesítést igénylő küldeményt a törvényes képviselőnek vagy a gondnoknak kell kézbesíteni. A gondnoknak e minőségét jogerős bírósági ítélettel vagy hatósági határozattal kell igazolnia. Az életkora miatt cselekvőképtelen természetes személy részére címzett küldeményt a törvényes képviselő címzettként veheti át.

(3) A postai szolgáltató a postai küldemény kézbesítését érintő, a címzettel vagy az egyéb jogosult átvevővel kapcsolatos információt tartalmazó bejelentést vagy nyilatkozatot - kivéve, ha annak valódisága kétséges - legalább a következő feltételek megléte esetén fogadja el:

a) a bejelentés személyesen és írásban, magyar nyelven történik, és
b) a bejelentő a bejelentés valódiságát
  ba) okirattal igazolja és az okirat eredetijét vagy eredetijének bemutatásával egyidejűleg másolatát csatolja,
  bb) okirat hiányában a bejelentésen nyilatkozik, hogy az abban foglaltak a valóságnak megfelelnek,
c) és a bejelentés tartalmazza a bejelentő aláírását és természetes személyazonosító adatait.

(4) A (3) bekezdés szerinti bejelentéssel vagy nyilatkozattal kapcsolatos eljárás, valamint a nyilatkozat alkalmazásának részletes szabályait a postai szolgáltató általános szerződési feltételeiben állapíthatja meg.

13. A hivatalos iratokkal kapcsolatos szolgáltatások részletes szabályai

27. § A hivatalos iratok felvételét, szükség szerint gyűjtését, feldolgozását, szállítását és kézbesítését együttesen vagy részben magában foglaló, gazdasági tevékenység keretében végzett szolgáltatás vonatkozásában e rendelet szabályait ezen alcímben foglalt eltérésekkel kell alkalmazni.

28. § (1) A hivatalos irat tértivevénye vagy az annak megfelelő elektronikus dokumentum előállításáról a feladó a saját költségén köteles gondoskodni. A feladónak a tértivevényen minden

esetben meg kell jelölnie, hogy sikertelen személyes kézbesítési kísérlet esetében milyen adattartalmú értesítést kell a címzett részére hátrahagyni.

(2) A hivatalos irat feladásához rendszeresített kötelezően alkalmazandó belföldi és nemzetközi tértivevény vagy az annak megfelelő elektronikus dokumentum tartalmi és formai követelményeit az Egyetemes Postai Közszolgáltatási Szerződés tartalmazza.

29. § (1) A hivatalos iratot a címzettnek vagy az egyéb jogosult átvevőnek személyes átadással kell kézbesíteni.

(2) Hivatalos irat a feladóval kötött egyedi szerződés vagy az általános szerződési feltételek szerinti külön rendelkezés alapján sem kézbesíthető alkalmi átvevőnek, a 15. § (3) bekezdés *a)* és *c)* pontja szerinti képviselőnek, valamint a 16. § (3) bekezdés *b)* pontja szerinti helyettes átvevőknek.

30. § (1) Hivatalos irat kézbesítésekor a küldemény átadásának igazolásaként a kézbesítési okiraton vagy az aláírást rögzítő egyéb technikai eszközön az átvevő személyazonosságát igazoló okmány elnevezésének, betűjelének és számának, az átvétel jogcímének - kivéve, ha a küldeményt a címzett veszi át - feltüntetésén, valamint az átvevő saját kezű aláírásán túl szerepelnie kell az átvevő személy olvasható nevének is.

(2) Nemzetközi viszonylatú hivatalos irat belföldi kézbesítése során a kézbesítési okiraton vagy az aláírást rögzítő egyéb technikai eszközön az (1) bekezdésben foglalt adatok mellett az átvevő lakcímét is fel kell tüntetni.

31. § (1) Amennyiben az első kézbesítési kísérlet nem vezetett eredményre - kivéve, ha az átvételt a címzett megtagadta, vagy a postai szolgáltató a 26. § (3) bekezdése szerinti kézbesítést érintő információval rendelkezik -, a postai szolgáltató a hivatalos irat érkezéséről és a sikertelen kézbesítési kísérletről a címzett részére a (3) bekezdésben meghatározott adattartalommal bíró értesítőt hagy hátra, a hivatalos iratot az értesítőn megjelölt kézbesítési ponton a címzett vagy egyéb jogosult átvevő rendelkezésére tartja, és a kézbesítést a sikertelen kézbesítés napját követő ötödik munkanapon újból megkísérli.

(2) A második kézbesítési kísérlet sikertelensége esetén a postai szolgáltató a címzett részére a (3) bekezdésben meghatározott adattartalommal bíró értesítőt hagy hátra, a hivatalos iratot az értesítőn megjelölt kézbesítési ponton a második kézbesítési kísérlet napját követő öt munkanapig a címzett vagy egyéb jogosult átvevő rendelkezésére tartja.

(3) Az értesítőnek tartalmaznia kell:

a) az „értesítés hivatalos irat érkezéséről” kifejezést és az értesítésnek a feladó által meghatározott típusát - az értesítő fejrészén,
b) a hivatalos iratot feladó szervezet nevét és a feladó szerinti település nevét,
c) a hivatalos iraton megjelölt címzett nevét és a küldeményen feltüntetett kézbesítési címet,
d) annak megjelölését, hogy hányadik sikertelen kézbesítési kísérletet követően került elhelyezésre az értesítő,

e) a sikertelen kézbesítési kísérlet napjának megjelölését,
f) a hivatalos irat azonosítására alkalmas jelzést,
g) annak a kézbesítési pontnak a megjelölését, ahol a jogosult átvevő a küldeményt átveheti,
h) a rendelkezésre tartás kezdő és végső időpontjának megjelölését - órára pontosan,
i) a küldemény átvételére való jogosultság e rendeletben meghatározott jogcímeit és a jogosultság igazolásának módját, arra való figyelmeztetést, ha a címzett a küldeményt csak saját maga veheti át,
j) az első kézbesítési kísérletet követően elhelyezett értesítőn annak megjelölését, hogy mely napon történik meg a második kézbesítési kísérlet,
k) a küldemény kézbesítési kísérletét végző kézbesítő olvasható nevét vagy a személyazonossága azonosítását lehetővé tévő egyéb jelzést, a kézbesítő aláírását,
l) az egyes hivatalos irat típusokra vonatkozóan az átvétel elmaradásának jogkövetkezményére figyelmeztető tartalom elérhetőségét.

(4) A második értesítőben megjelölt átvételi határidő eredménytelen elteltét követő munkanapon a postai szolgáltató a hivatalos iratot a tértivevényen feltüntetendő „nem kereste” jelzéssel a feladónak visszaküldi.

(5) A postafiókra címzett hivatalos irat érkezéséről az egyetemes postai szolgáltató a fiókban elhelyezett (1)-(2) bekezdés szerinti értesítővel ad tájékoztatást, abban az esetben is, ha a hivatalos irat postafiókra címzett, de nem a postafiók bérlőjének szól.

32. § (1) Az egyetemes postai szolgáltató a címzett eltérő rendelkezése esetén is köteles a hivatalos iratot a címzett - utánküldés szolgáltatás igénybevétele alapján a nyilvántartásában szereplő - új belföldi címére továbbítani az utánküldés szolgáltatásra vonatkozó szerződés hatálya alatt.

(2) A postai szolgáltató abban az esetben is hátrahagyja a címzett számára a 31. § (1)-(2) bekezdése szerinti értesítőt, ha a hivatalos irat átvételétől a meghatalmazott zárkózik el.

9/2005. (I. 19.) Korm. rendelet a postai szolgáltatók, a postai közreműködők és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének részletes szabályairól

http://njt.hu/cgi_bin/njt_doc.cgi?docid=93020.269245

1. § (1) E rendelet hatálya a titkos információgyűjtésre és a titkos adatszerzésre (a továbbiakban együtt: titkos információgyűjtés), valamint az ezzel összefüggő tevékenységek végzésére - külön törvényben - felhatalmazott szervezetekre és a postai szolgáltatást végzőkre (a továbbiakban: a postai szolgáltató), a postai közreműködőkre, valamint a Nemzeti Hírközlési Hatóságra (a továbbiakban: Hatóság) terjed ki.

(2) Az (1) bekezdésben megjelölt szervezetek közötti együttműködésre e rendelet rendelkezéseit kell alkalmazni, amennyiben a titkos információgyűjtés végrehajtása a postai szolgáltatásokról szóló 2012. évi CLIX. törvényben (a továbbiakban: Postatv.) meghatározott postai tevékenységet érinti.

A titkos információgyűjtés feltételeinek biztosítása

2. § (1) A Hatóság a postai szolgáltató által a Postatv. 11. §-a alapján benyújtott kérelemről, illetve a postai szolgáltatótól a Postatv. 10. § (1) bekezdése alapján érkezett bejelentésről, valamint a Postatv. 13. § (1) bekezdésében, illetve 13. § (2) bekezdésében szabályozott bejelentésekről 15 napon belül tájékoztatja a Nemzetbiztonsági Szakszolgálatot (a továbbiakban: NBSZ).

(2) A postai szolgáltató az NBSZ kérésére köteles megadni mindazokat az adatokat, információkat, amelyek a titkos információgyűjtés eszközeinek és módszereinek alkalmazásához, valamint az ezzel összefüggő feladatok ellátásához szükségesek.

3. § A postai szolgáltató köteles az NBSZ erre vonatkozó előzetes igénye esetén a titkos információgyűjtés feladatainak végrehajtására megfelelő zárt helyiséget rendelkezésre bocsátani, és biztosítani, hogy abba az NBSZ kijelölt munkatársai - a szolgáltató munkaidejében bármikor - beléphessenek, ott szükség szerint munkát végezzenek, a titkos információgyűjtéshez szükséges eszközöket használjanak.

4. § (1) A postai szolgáltató és a postai közreműködő technológiai és logisztikai hálózati rendszer-, illetve szolgáltatásfejlesztési elképzeléseit, terveit köteles egyeztetni az NBSZ-szel annak érdekében, hogy a fejlesztések ne akadályozzák, vagy ne tegyék lehetetlenné a titkos információgyűjtést.

(2) A postai szolgáltató nem alkalmazhat közreműködőt olyan módon, amely a titkos információgyűjtést kizárja vagy ellehetetleníti.

Az igazságügyért felelős miniszter vagy bíró engedélyéhez nem kötött titkos információgyűjtés eljárási rendje

5. § (1) Az igazságügyért felelős miniszter vagy bíró engedélyéhez nem kötött titkos információgyűjtés során a titkos információgyűjtésre felhatalmazott szervezetek - a rájuk vonatkozó törvényi rendelkezéseknek megfelelően, figyelemmel az információs önrendelkezési jogról és az információszabadságról szóló törvény előírásaira - közvetlenül és az NBSZ-en keresztül is jogosultak a Postatv. 54. § (1) bekezdése szerinti adatok megkérésére.

(2) Az (1) bekezdésben foglaltak alkalmazásának jogszerű végrehajtásáért az ügyben eljáró titkos információgyűjtésre felhatalmazott szervezet a felelős.

Az igazságügyért felelős miniszter vagy bíró engedélyéhez kötött titkos információgyűjtés eljárási rendje

6. § (1) Amennyiben a titkos információgyűjtés eszközeinek, illetve módszereinek postai szolgáltatónál történő alkalmazásához az igazságügyért felelős miniszter vagy bíró engedélye szükséges, a titkos információgyűjtésre felhatalmazott szervezetek igényeinek kielégítését - külön törvényben meghatározott feltételek mellett - az NBSZ látja el. Az eszköz, illetve módszer alkalmazási feltételeinek biztosítását a postai szolgáltatótól írásban kell megrendelni.

(2) Az (1) bekezdésben említett titkos információgyűjtő eszközök, módszerek alkalmazási feltételeinek biztosítását a postai szolgáltatótól kizárólag az NBSZ igényelheti, és ezekben az esetekben a megszerzett adatokat, információkat és küldeményeket a szolgáltató az NBSZ-en kívül más személynek nem adhatja át, illetve más számára nem teheti hozzáférhetővé.

(3) A külön törvényekben meghatározott kivételes engedélyezés, illetve sürgősségi, valamint halaszthatatlan elrendelés alapján azonnali intézkedést igénylő esetekben a postai szolgáltatónak szóban is továbbítható megrendelés, amelyet haladéktalanul írásban is meg kell erősíteni, vagy le kell mondani. Ha a postai szolgáltató az NBSZ által szóban továbbított megrendelésnek írásba foglalt megerősítését az azt követő első munkanapon nem kapja meg, erről az NBSZ-t írásban haladéktalanul tájékoztatja, és a konkrét feladat végrehajtásában a további közreműködést megtagadja.

(4) A külön törvényben meghatározott engedély beszerzéséért és az alkalmazás jogszerűségéért a titkos információgyűjtésre felhatalmazott szervezet, míg az engedélyben foglaltak szakszerű végrehajtásáért az NBSZ a felelős.

A költségviselés szabályai

7. § A titkos információgyűjtésre felhatalmazott szervek részére a Postatv. 54. § (1) bekezdésében meghatározott adatokból történő adatszolgáltatás, a Postatv. 55. § (6) bekezdése szerinti szolgáltatás, valamint a titkos információgyűjtés feltételeinek biztosítása a Postatv. 38. §-a alapján díj-, költség- és térítésmentes.

Az adat- és titokvédelemre vonatkozó rendelkezések

8. § (1) Az e rendelet alapján a postai szolgáltatóval való együttműködés során végzett titkos információgyűjtéssel, annak eszközével és módszerével, valamint azok alkalmazásával összefüggő valamennyi, továbbá a Postatv. 38. §-ában, illetve 55. § (6) bekezdésében meghatározottakra vonatkozó adatot a minősített adat védelméről szóló jogszabályok alapján kell minősíteni, és azok szerint kell kezelni.

(2) A postai szolgáltató és a titkos információgyűjtésre felhatalmazott szervezet - amennyiben az együttműködés tartalma szükségszerűen igényli minősített adatok átadását - titokvédelmi

szerződést (a továbbiakban: szerződés) köt a minősített adatok átadásának és kezelésének feltételeiről.

(3) A szerződés megkötését a titkos információgyűjtésre felhatalmazott szervezet kezdeményezheti. A kezdeményezéstől számított 30 napon belül a szerződést meg kell kötni.

(4) A szerződésben a (2) bekezdésben meghatározottakon túlmenően rögzíteni kell azt is, hogy a postai szolgáltató az általa a titkos információgyűjtés végzésével összefüggésben megismert minősített adatot kizárólag a hatályos jogszabályoknak megfelelő feltételekkel és módon továbbíthatja külföldre.

(5) A szerződés kiterjedhet az együttműködést érintő egyéb rendelkezésekre is.

9. § A titkos információgyűjtésre felhatalmazott szervezetek a postai szolgáltató számára csak azokat az adatokat továbbíthatják, amelyek a titkos információgyűjtés végrehajtása érdekében a postai szolgáltatóra háruló kötelezettségek teljesítéséhez elengedhetetlenül szükségesek.

10. § A postai szolgáltató köteles meg-, illetve visszaküldeni a titkos információgyűjtés során vagy céljából keletkezett adatokat tartalmazó, e célra fenntartott adathordozók valamennyi példányát a titkos információgyűjtésre felhatalmazott szervezetnek, illetve köteles az adatok átadása után a saját rendszerében keletkezett adatok visszavonhatatlan törléséről gondoskodni. Ezekről az adatokról másolatot nem készíthet, és másodpéldányt nem tárolhat. Nem jogosult továbbá a titkos információgyűjtéssel összefüggésben tudomására jutott, birtokába került adatok gyűjtésére, archiválására.

11. § (1) A postai szolgáltató alkalmazottai abban az esetben vonhatóak be a titkos információgyűjtésre felhatalmazott szervezetek részére végzett szolgáltatás teljesítésébe, ha a titkos információgyűjtés műszaki eszközökkel vagy egyéb műszaki jellegű megoldással nem valósítható meg.

(2) A postai szolgáltató alkalmazottainak bevonása esetén a postai szolgáltató kötelezettsége olyan technológiai, szervezeti megoldás alkalmazása, amely postai tevékenység végrehajtásával leplezi a titkos információgyűjtés alkalmazásának támogatását.

(3) A titkos információgyűjtéssel összefüggő tevékenység végzésében - amennyiben az szükségszerűen együtt jár minősített adatok megismerésével - a postai szolgáltatónak csak azok az alkalmazottai vehetnek részt, akik a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott, a minősítésnek megfelelő szintű nemzetbiztonsági ellenőrzésen megfeleltek, betekintési jogosultsággal rendelkeznek és titoktartási nyilatkozatot tettek.

(4) A postai szolgáltató az igényelt szolgáltatás teljesítésébe bevont alkalmazottai részére olyan feladatkört és jogosultságot köteles biztosítani, amely lehetővé teszi e tevékenység titkos - a titkos információgyűjtésre felhatalmazott szervezet törvényes igényeinek megfelelő -, késedelem nélküli ellátását.

12. § A postai szolgáltató köteles gondoskodni a titkos információgyűjtéssel összefüggő, a postai küldemények feldolgozását végző technikai rendszerekhez, az abban tárolt adatokhoz, valamint a titkos információgyűjtés eszközéhez, illetve konkrét módszeréhez való illetéktelen hozzáférés kizárásáról.

Az együttműködés részletes szabályai

13. § (1) A titkos információgyűjtésre felhatalmazott szervezetek a Postatv. és az e rendeletben foglalt feladatok teljesítésére vonatkozó részletszabályok meghatározása érdekében a postai szolgáltatóval írásbeli együttműködési megállapodás (a továbbiakban: megállapodás) megkötését kezdeményezhetik.

(2) Kezdeményezés esetén a postai szolgáltató köteles a kezdeményezéstől számított 60 napon belül megkötni a megállapodást. A megállapodás tartalmát a titkos információgyűjtésre felhatalmazott szervezet tevékenységének jellegére tekintettel az együttműködő felek határozzák meg.

(3) Az NBSZ-szel kötendő megállapodásnak tartalmazni kell:

a) a titkos információgyűjtés keretében a külön törvényekben meghatározott engedély alapján megrendelt szolgáltatás igénylésének, az igény teljesítésének módját és rendjét, ezen belül az e rendelet 3. §-ában meghatározott zárt helyiség biztosításának követelményeit, valamint feltételeit;
b) a kapcsolattartás szintjét és módját;
c) a postai technológiai, logisztikai-hálózati rendszer- és szolgáltatásfejlesztéssel kapcsolatos tájékoztatási és egyeztetési eljárás szabályait;
d) az adat- és titokvédelmi szabályok érvényesítésének módját;
e) a postai szolgáltató részéről közreműködő alkalmazottak kiválasztásának, egyeztetésének, ellenőrzésének rendjét;
f) az együttműködési megállapodásban foglaltak teljesülésének, szükség szerinti közös értékelésének és felülvizsgálatának rendjét;
g) minden olyan feltételt, eljárást, amelyet az *a)-f)* pontokon túlmenően az együttműködő felek szükségesnek tartanak.

14. § Amennyiben a felek valamelyik együttműködési kérdésben nem tudnak megállapodni, úgy bármelyikük kérheti a Hatóság Tanácsának Elnökétől egyeztetési eljárás lefolytatását.

15. § A titkos információgyűjtésre felhatalmazott szervezetek a külön törvényben meghatározott feladataik ellátása érdekében a postai szolgáltató alkalmazási feltételeinek egyébként megfelelő alkalmazottjuk foglalkoztatása céljából - külön megállapodásban meghatározott időtartamra és feltételekkel - munkaviszony létesítését kezdeményezhetik a postai szolgáltatóknál.

Jogkövetkezmények

16. § (1) E rendeletben foglalt kötelezettségek postai szolgáltatónak felróható okból történő megsértése esetén a Postatv. 68. §-ában foglaltak alkalmazandóak. A kötelezettségek megsértéséről a titkos információgyűjtésre felhatalmazott szervezet tájékoztatja a Hatóság Tanácsának Elnökét.

(2) Amennyiben a titokvédelmi szerződés a 8. § (3) bekezdésében, valamint az együttműködési megállapodás a 13. § (2) bekezdésében meghatározott határidőben - a postai szolgáltatónak felróható okból - nem kerül megkötésre, erről a titkos információgyűjtésre felhatalmazott szervezet tájékoztatja a Hatóság Tanácsának Elnökét.

(3) Amennyiben a postai szolgáltató a Hatóság Tanácsának Elnöke által meghozott, a 14. §-ban meghatározott egyeztetési eljárást lezáró határozatában foglaltakat nem teljesíti, vele szemben a Hatóság az (1) bekezdésben foglaltak alapján jár el.

17. § (1) Amennyiben a postai szolgáltató a Postatv. 36. § (1) bekezdése alapján a postai tevékenység ellátásához közreműködőt vesz igénybe, a közreműködő kiválasztásakor köteles figyelemmel lenni a titkos információgyűjtés feltételeinek folyamatos biztosítására.

(2) A Postatv. 38. §-ában, illetve 55. § (6) bekezdésében alapján a postai közreműködő köteles elősegíteni a titkos információgyűjtéssel összefüggésben a vele közvetlen kapcsolatban álló postai szolgáltató számára meghatározott kötelezettségek teljesítését.

2016. évi CXXX. törvény a polgári perrendtartásról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=198992.338822

XXII. FEJEZET
OKIRATOK

93. Bizonyítás okirattal

320. § *[Az okirat rendelkezésre bocsátása]*

(1) Ha a fél tényállításait okirattal kívánja bizonyítani, az okiratot beadványához kell csatolnia vagy a tárgyaláson be kell mutatnia. Idegen nyelvű okirathoz csatolni kell annak legalább egyszerű magyar nyelvű fordítását is. Ha a lefordított szöveg helyessége, illetve teljessége tekintetében kétely merül fel, hiteles fordítást kell alkalmazni; ennek hiányában az okiratot a bíróság figyelmen kívül hagyja.

(2) A bíróság a bizonyító fél kérelmére az ellenérdekű felet kötelezheti a birtokában lévő olyan okirat rendelkezésre bocsátására, amelyet a polgári jog szabályai szerint egyébként is köteles kiadni vagy bemutatni. Ilyen kötelezettség az ellenérdekű felet különösen akkor terheli, ha az okiratot a bizonyító fél érdekében állították ki, vagy az rá vonatkozó jogviszonyt tanúsít, vagy ilyen jogviszonnyal kapcsolatos tárgyalásra vonatkozik.

(3) Ha az okirat olyan személy birtokában van, aki a perben nem vesz részt, a bíróság a szemlére vonatkozó szabályok alkalmazásával intézkedik az okirat beszerzése iránt.

(4) Ha az okiratnak a bíróság hivatalos helyiségében történő rendelkezésre bocsátása lehetetlen vagy aránytalanul nehéz, az okiratot a bíróság a szemle szabályainak megfelelő alkalmazásával a helyszínen szemléli meg.

(5) Olyan tényre vonatkozóan, amely okirattal bizonyítható, a bíróság az egyéb bizonyítást mellőzheti.

321. § *[Eredeti okirat, másolat, kivonat]*

(1) Az eredeti okirat helyett annak hiteles vagy egyszerű másolatban történő rendelkezésre bocsátása is elegendő, ha ezt az ellenérdekű fél nem kifogásolja, és az eredeti okirat rendelkezésre bocsátását a bíróság sem tartja szükségesnek.

(2) Ha a bizonyító fél által rendelkezésre bocsátott, az eredeti okiratról készített okirat (másolat, felvétel, adathordozó útján készített okirat) teljes bizonyító erejű magánokiratnak vagy közokiratnak minősül, a bíróság az ellenérdekű fél terhére értékeli, ha az ellenbizonyítás során a birtokában lévő eredeti okiratot nem bocsátja rendelkezésre.

(3) Ha könyvnek vagy egyéb nagyobb terjedelmű okiratnak csak egy része szolgál bizonyítékul, elegendő csupán ezt a részt mint kivonatot rendelkezésre bocsátani, kivéve, ha a bíróság megítélése szerint bármely okból az okirat teljes terjedelmű rendelkezésre bocsátása szükséges.

(4) A bíróság elrendelheti, hogy az eredeti okiratot vagy az arról készített másolatot, kivonatot az iratokhoz csatolják; ha fontosabb eredeti okiratot kell az iratokhoz csatolni, a bíróság gondoskodik annak megőrzéséről.

(5) Az iratokhoz csatolt okiratok és egyéb mellékletek kiadásáról a bíróság - szükség esetén az érdekeltek meghallgatása után - dönt. Ha a bíróság szükségesnek tartja, az okirat vagy egyéb melléklet kiadását egyszerű vagy hiteles másolat csatolásától teheti függővé.

322. § *[Irat- és adatbeszerzés]*

(1) Bíróságnál, közjegyzőnél, más hatóságnál, közigazgatási szervnél vagy valamely szervezetnél lévő irat, illetve adat beszerzése iránt a fél bizonyítási indítványára a bíróság intézkedik, ha az irat, illetve adat kiadását a fél közvetlenül nem kérheti. Az eredeti okirat beszerzése mellőzhető, ha annak megtekintésére nincs szükség és a fél a tárgyaláson annak hiteles vagy egyszerű másolatát bemutatja. Az okirat megküldése csak akkor tagadható meg, ha az minősített adatot tartalmaz. A közreműködő eljárási kötelezettsége megszegése esetén csak a 272. § (1) bekezdés b) pontja szerinti kényszerítő eszköz alkalmazásának van helye.

(2) Ha a rendelkezésre bocsátott okirat az azt megküldő nyilatkozata szerint olyan minősített adatot, üzleti titkot, hivatásbeli titkot vagy törvényben meghatározott más titkot tartalmaz, amelynek felhasználásához a minősítő vagy a titoktartás alóli felmentés megadására jogosult (a továbbiakban: titokgazda) nem járult hozzá, a bíróság megkeresi a minősítőt vagy a titokgazdát a minősített adat vagy titok megismerésének engedélyezése céljából, kivéve, ha az okirat tartalma törvény rendelkezése alapján nem minősül üzleti titoknak, vagy a per tárgya annak az eldöntése, hogy az okirat tartalma közérdekű adatnak minősül-e.

(3) Ha a titokgazda a megkeresés átvételétől számított nyolc napon belül nem nyilatkozik, megadottnak kell tekinteni az engedélyt; erre a titokgazdát figyelmeztetni kell. Egyebekben a tanúvallomás megtagadására vonatkozó szabályokat kell alkalmazni. Ha a titokgazda határidőn belül úgy nyilatkozik, hogy nem járul hozzá az üzleti, hivatásbeli vagy törvényben meghatározott más titok felek általi megismeréséhez, az okiratnak ez a része nem használható fel bizonyítékként.

(4) A bíróság az iratok beérkezéséről, valamint - a titokgazda esetleges nyilatkozatától függően - az iratok megismerhetőségéről, illetve perben történő felhasználhatóságáról a feleket tájékoztatja.

(5) A perben nem használható fel bizonyítékként az a minősített adatot tartalmazó okirat, illetve okiratrész, melynek a fél általi megismeréséhez a minősítő nem járult hozzá.

(6) Az (5) bekezdés nem alkalmazható, ha a pert a megismerési engedély megtagadása miatt indították, vagy a per tárgya annak eldöntése, hogy az okirat tartalma minősített adatnak minősüle. Az ilyen perben a felperes, a felperes oldalán beavatkozó személy és ezek képviselője a minősített adatot az eljárás során nem ismerheti meg. A perben részt vevő egyéb személyek, valamint azok képviselői a minősített adatot csak akkor ismerhetik meg, ha a nemzetbiztonsági ellenőrzésüket elvégezték.

(7) A bíróság gondoskodik arról, hogy az e §-ban nem nevesített, törvény által védett egyéb adat ne kerüljön nyilvánosságra, ne juthasson illetéktelen személy tudomására, az adat törvényben meghatározott védelme a bíróság eljárásában is biztosított legyen.

(8) A bíróság az (1) bekezdésben foglaltak iránt az ellenkérelem előterjesztését követően a perfelvétel során is intézkedhet.

94. Az okiratok fajtái

323. § *[A közokirat]*

(1) A közokirat olyan papír alapú vagy elektronikus okirat, amelyet bíróság, közjegyző vagy más hatóság, illetve közigazgatási szerv ügykörén belül, a jogszabályi rendelkezéseknek megfelelő módon állított ki.

(2) A közokiratot az ellenkező bizonyításáig valódinak kell tekinteni, a bíróság azonban az okirat kiállítóját hivatalból is felhívhatja nyilatkozattételre az okirat valódisága tekintetében.

(3) A közokirat teljes bizonyító erővel bizonyítja

a) hogy a kiállító a benne foglalt intézkedést megtette vagy határozatot a benne foglalt tartalommal meghozta,
b) a közokirattal tanúsított adatok és tények valóságát,
c) a közokiratban foglalt nyilatkozat megtételét, annak idejét és módját.

(4) Elektronikus közokirat kiállításához az is szükséges, hogy a közokirat kiállítására jogosult az elektronikus okiraton - ha jogszabály eltérően nem rendelkezik - minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást vagy bélyegzőt, és amennyiben jogszabály így rendelkezik időbélyegzőt helyezzen el.

(5) Jogszabály egyéb okiratot vagy - adathordozótól függetlenül - más dolgot közokirattá nyilváníthat.

(6) Közokirattal szemben is van helye ellenbizonyításnak, kivéve, ha azt törvény kizárja vagy korlátozza.

324. § *[A közokiratról készült másolat bizonyító ereje]*

(1) Az eredeti közokiratéval azonos bizonyító ereje van a közokiratról készített másolatnak - a másolatkészítés technológiájától és adathordozótól függetlenül -, ha a másolatot közokirat

kiállítására jogosult vagy megőrzésére hivatott szerv, továbbá ha ezek ellenőrzése mellett más személy vagy szervezet készítette, valamint, ha azt az E-ügyintézési tv. szerinti hiteles másolatkészítés központi elektronikus ügyintézési szolgáltatás szabályai szerint készítették.

(2) Ha közokiratnak nem minősülő okiratról készül közokiratba foglalt másolat, a közokirat csupán azt bizonyítja, hogy annak tartalma a közokiratnak nem minősülő eredeti okiratéval megegyezik.

325. § *[A teljes bizonyító erejű magánokirat]*

(1) Teljes bizonyító erejű a magánokirat, ha

a) a kiállító az okiratot saját kezűleg írta és aláírta,

b) két tanú igazolja, hogy az okirat aláírója a részben vagy egészben nem általa írt okiratot előttük írta alá, vagy aláírását előttük saját kezű aláírásának ismerte el; igazolásként az okiratot mindkét tanú aláírja, továbbá az okiraton a tanúk nevét és lakóhelyét - ennek hiányában tartózkodási helyét - olvashatóan is fel kell tüntetni,

c) az okirat aláírójának aláírását vagy kézjegyét az okiraton bíró vagy közjegyző hitelesíti,

d) az okiratot a jogi személy képviseletére jogosult személy a rá vonatkozó szabályok szerint megfelelően aláírja,

e) ügyvéd vagy kamarai jogtanácsos az általa készített okirat szabályszerű ellenjegyzésével bizonyítja, hogy az okirat aláírója a más által írt okiratot előtte írta alá vagy aláírását előtte saját kezű aláírásának ismerte el,

f) az elektronikus okiraton az aláíró a minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírását vagy bélyegzőjét helyezte el, és - amennyiben jogszabály úgy rendelkezik - azon időbélyegzőt helyez el,

g) az elektronikus okiratot az aláíró a Kormány rendeletében meghatározott azonosításra visszavezetett dokumentumhitelesítés szolgáltatással hitelesíti, vagy

h) olyan, törvényben vagy kormányrendeletben meghatározott szolgáltatás keretében jött létre, ahol a szolgáltató az okiratot a kiállító azonosításán keresztül a kiállító személyéhez rendeli és a személyhez rendelést a kiállító saját kezű aláírására egyértelműen visszavezethető adattal együtt vagy az alapján hitelesen igazolja; továbbá a szolgáltató az egyértelmű személyhez rendelésről kiállított igazolást elektronikus dokumentumba kapcsolt, elválaszthatatlan záradékba foglalja és azt az okirattal együtt legalább fokozott biztonságú elektronikus bélyegzővel és legalább fokozott biztonságú időbélyegzővel látja el.

(2) Ha az okirat aláírója nem tud olvasni, illetve nem érti azt a nyelvet, amelyen az okirat készült, csak akkor jön létre teljes bizonyító erejű magánokirat, ha magából az okiratból kitűnik, hogy annak tartalmát a tanúk egyike vagy a hitelesítő személy az okirat aláírójának megmagyarázta.

(3) A teljes bizonyító erejű magánokirat az ellenkező bizonyításáig teljes bizonyító erővel bizonyítja, hogy az okirat aláírója az abban foglalt nyilatkozatot megtette, illetve elfogadta vagy magára kötelezőnek ismerte el.

(4) A teljes bizonyító erejű magánokirat valódiságát csak akkor kell bizonyítani, ha azt az ellenfél kétségbe vonja, vagy a valódiság bizonyítását a bíróság szükségesnek találja.

(5) Ha a teljes bizonyító erejű magánokiraton szereplő aláírás valódisága nem vitás vagy bizonyított, illetve a legalább fokozott biztonságú elektronikus aláírás vagy bélyegző vagy zárt rendszerben alkalmazott bizalmi szolgáltatás keretében a kiállító saját kezű aláírására egyértelműen visszavezethető adatok ellenőrzésének eredményéből más nem következik, az aláírást vagy a bélyegzőt megelőző szöveget - elektronikus okirat esetén az aláírt vagy bélyegzővel ellátott adatokat - az ellenkező bizonyításáig meg nem hamisítottnak kell tekinteni, kivéve, ha az okiratnak olyan rendellenességei vagy hiányai vannak, amelyek e vélelmet megdöntik.

(6) A teljes bizonyító erejű magánokiraton szereplő aláírás valódiságát vagy a szöveg meg nem hamisított voltát - kétség esetén - más olyan írással való összehasonlítás útján is meg lehet állapítani, amelynek valódisága nem kétséges. A bíróság ennek érdekében íráspróbát is elrendelhet, és szükség esetén annak eredményét, illetve a vitatott okiratot, aláírást szakértővel is megvizsgáltathatja.

(7) Ha a legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel ellátott elektronikus okirat aláírójának vagy bélyegző létrehozójának azonossága, illetve az okirat hamisítatlansága kétséges, ezek megállapítása érdekében a bíróság elsősorban az elektronikus aláíráshoz vagy bélyegzőhöz tartozó tanúsítványt kibocsátó bizalmi szolgáltatót keresi meg. Az elektronikus okirathoz kapcsolt időbélyegző által igazolt adatokkal kapcsolatos kétség esetén a bíróság elsősorban az időbélyegzést végző bizalmi szolgáltatót keresi meg. Az olyan zárt rendszerben alkalmazott bizalmi szolgáltatás keretében kiállított elektronikus okirat esetén, ahol a szolgáltató az okiratot a kiállító személyéhez rendeli és a személyhez rendelést a kiállító saját kezű aláírására egyértelműen visszavezethető adatokkal együtt hitelesen igazolja, a bíróság elsősorban a zárt rendszer bizalmi szolgáltatóját keresi meg.

(8) Az elektronikus okirat esetén az aláírt vagy bélyegzővel ellátott adatokat az ellenkező bizonyításáig meg nem hamisítottnak kell tekinteni a tárolást végző szolgáltató igazolása alapján, ha a szolgáltató

a) a tárolásra átvételkor meggyőződött az elektronikus dokumentum hitelesítésének érvényességéről,

b) a tárolást a Kormány rendeletében meghatározott feltételeknek megfelelő, az E-ügyintézési tv. szerinti minősített archiválási szolgáltatás vagy elektronikus dokumentumtárolás központi elektronikus ügyintézési szolgáltatás keretében végzi, és

c) a Kormány rendeletében meghatározottak szerint igazolja az elektronikus okirat hitelességét.

326. § *[Az egyszerű magánokirat]*

A magánokirathoz - ha azt nem a 325. § (1) bekezdése szerint állították ki - nem fűződik törvényi vélelem, és annak bizonyító erejét a bíróság a bizonyítás általános szabályai szerint a tárgyalás és a bizonyítás összes adatának figyelembevételével állapítja meg, kivéve, ha jogszabály

a) adott magánokirat bizonyító erejét másként szabályozza, vagy

b) az okirati bizonyításhoz meghatározott alakban kiállított okiratot ír elő.

327. § *[A jogi személy által kiállított vagy őrzött okiratról készült másolat bizonyító ereje]*

A jogi személy által kiállított vagy őrzött okiratról készített papír alapú vagy elektronikus másolat teljes bizonyító erővel bizonyítja, hogy tartalma megegyezik az eredeti okiratéval, feltéve, hogy a jogi személy, amely az okiratot kiállította vagy azt őrzi, ezt szabályszerűen igazolta a 325. § (1) bekezdés d) vagy f) pontjának megfelelő másolat kiállításával. A jogi személy által készített másolat bizonyító ereje az eredeti okiratéval azonos, kivéve, ha a másolat közokiratról készült.

XLVI. FEJEZET
AZ ELEKTRONIKUS KAPCSOLATTARTÁS

156. A törvény rendelkezéseinek alkalmazása elektronikus kapcsolattartás esetén, valamint az elektronikus kapcsolattartás igénybevétele

604. § *[Utaló szabály]*

E törvény rendelkezéseit az elektronikus kapcsolattartás során az e fejezetben foglalt eltérésekkel kell alkalmazni.

605. § *[Választható elektronikus kapcsolattartás]*

(1) A perben az elektronikus kapcsolattartásra nem köteles fél vagy a jogi képviselőnek nem minősülő képviselője - az (5) bekezdésben foglalt kivétellel - a keresetlevelet, továbbá minden egyéb beadványt és ezek mellékletét, valamint okiratot (e fejezetben a továbbiakban együtt: beadvány) választása szerint elektronikus úton is benyújthatja, az E-ügyintézési tv.-ben és végrehajtási rendeleteiben meghatározott módon.

(2) Az elektronikus úton történő kapcsolattartásra vonatkozó bejelentést a fél vagy a képviselő az eljárás bármely szakaszában megteheti az eljáró bíróságnál. A beadvány elektronikus úton történő benyújtását az (1) bekezdés szerinti elektronikus út vállalásának kell tekinteni.

(3) Az (1) bekezdés szerinti elektronikus út választása esetén az eljárás folyamán - ideértve az eljárás minden szakaszát és a rendkívüli perorvoslatot is - a fél, illetve képviselője köteles a

bírósággal a kapcsolatot elektronikus úton tartani és a bíróság is valamennyi bírósági iratot elektronikusan kézbesít a részére.

(4) Ha a fél, illetve a nem jogi képviselőnek minősülő képviselője nem vállalja az elektronikus kézbesítést, de az elektronikus kézbesítés a másik fél számára kötelező vagy azt vállalta, a bíróság a papír alapú okiratot benyújtó fél, illetve képviselő beadványait digitalizálja és elektronikusan kézbesíti a másik fél számára.

(5) A bíróság a fél részére - feltéve, hogy az elektronikus kapcsolattartásra személyében nem köteles vagy azt nem vállalta - papír alapon kézbesíti a bírósági iratot, ha a fél az eljárásban jogi képviselője vagy elektronikus kapcsolattartást vállaló egyéb képviselője útján jár el és az iratot nem a képviselő, hanem a fél részére kell kézbesíteni, vagy a képviselő részére nem lehet kézbesíteni. A bíróság a felet tájékoztatja arról, hogy a bírósággal a kapcsolatot elektronikus úton is tarthatja.

606. § *[Áttérés papír alapú kapcsolattartásra]*

(1) Ha jogi képviselő nélkül eljáró fél vagy jogi képviselőnek nem minősülő képviselője vállalta, hogy a bírósággal a kapcsolatot elektronikus úton tartja, utóbb, a beadvány papír alapú benyújtásával egyidejűleg kérheti a bíróságtól a papír alapú eljárásra történő áttérés engedélyezését. A kérelemben valószínűsíteni kell, hogy a fél, illetve a jogi képviselőnek nem minősülő képviselő körülményeiben olyan változás következett be, amely miatt az elektronikus úton történő eljárás a továbbiakban számára aránytalan megterhelést jelentene.

(2) A papír alapú kapcsolattartásra történő áttérés engedélyezése esetén erről külön végzést hozni nem kell. Az áttérés iránti kérelem visszautasításáról vagy elutasításról szóló végzést a bíróság a féllel, illetve a jogi képviselőnek nem minősülő képviselővel papír alapon közli. A végzés ellen papír alapon is előterjeszthető fellebbezésnek van helye. A papír alapon benyújtott, az (1) bekezdés szerinti beadványt az áttérés iránti kérelem visszautasítása vagy elutasítása esetén is szabályszerűen benyújtott beadványnak kell tekinteni, azt - az ismételten hiányos vagy alaptalan áttérés iránti kérelem előterjesztésének esetét kivéve - elektronikus úton nem kell benyújtani.

(3) A papír alapú kapcsolattartásra történő áttérés iránti kérelem elutasítása esetén azonos okból ismételten áttérés iránti kérelmet nem lehet benyújtani, az ennek ellenére benyújtott áttérés iránti kérelmet a bíróság visszautasítja. Ha a jogi képviselő nélkül eljáró fél nyilvánvalóan alaptalanul terjeszt elő áttérés iránti kérelmet, az azt elutasító végzésben pénzbírsággal sújtható.

607. § *[Jogutódlás az elektronikus kapcsolattartásban]*

A jogi képviselő nélkül eljáró jogutód félre nem vonatkozik az, hogy a jogelőd az elektronikus kapcsolattartást vállalta, vagy a jogelőd tekintetében a papír alapú kézbesítésre történő áttérés megtörtént.

608. § *[Kötelező elektronikus kapcsolattartás]*

(1) Az E-ügyintézési tv. alapján elektronikus úton történő kapcsolattartásra kötelezett minden beadványt kizárólag elektronikusan - az E-ügyintézési tv.-ben és végrehajtási rendeleteiben meghatározott módon - nyújthat be a bírósághoz, és a bíróság is elektronikusan kézbesít a részére.

(2) E fejezet alkalmazása szempontjából jogi képviselőnek kell tekinteni a 75. § (1) bekezdésében meghatározott személyeket, valamint az ügyvédjelöltet és a jogi előadót, ha e törvény szerint a perben eljárhat.

157. Elektronikus kapcsolattartás a szakértővel, a bírósággal, a közigazgatási szervvel és más hatósággal

609. § *[Elektronikus kapcsolattartás a szakértővel]*

(1) Az E-ügyintézési tv. alapján elektronikus úton történő kapcsolattartásra nem kötelezett szakértő az igazságügyi szakértői névjegyzékbe történő bejelentéssel, az igazságügyi szakértői névjegyzékben nem szereplő - az E-ügyintézési tv. alapján elektronikus úton történő kapcsolattartásra nem kötelezett - szakértői tevékenységre jogszabályban feljogosított állami szerv, intézmény vagy szervezet (e fejezetben a továbbiakban együtt: szakértői tevékenységet végző szerv) az Országos Bírósági Hivatal részére történő bejelentéssel vállalhatja az elektronikus kapcsolattartást.

(2) Ha a szakértő és a szakértői tevékenységet végző szerv az E-ügyintézési tv. alapján elektronikus úton történő kapcsolattartásra köteles vagy azt az (1) bekezdés szerint vállalja - a (3) és (4) bekezdésben foglaltak kivételével - a szakvéleményét és egyéb beadványait az E-ügyintézési tv.-ben és végrehajtási rendeleteiben meghatározott módon, elektronikusan kézbesíti a bíróságnak és a bíróság is valamennyi bírósági iratot elektronikusan kézbesít a részére.

(3) A bíróság a szakértő, illetve a szakértői tevékenységet végző szerv indokolt kérelmére - a 613. § (3) bekezdésében meghatározott okból, kivételesen - elektronikus kapcsolattartás esetén is engedélyt adhat a szakvélemény vagy egy részének papír alapú benyújtására.

(4) A bíróság papír alapon vagy adathordozón bocsátja rendelkezésre a szakértő, illetve a szakértői tevékenységet végző szerv részére a bírósági irat mellékletét, ha az adathordozó jellegéből adódóan a digitalizálás lehetetlen, valamint ha a papír alapú okirat valódisága vitás vagy annak papír alapú megtekintése egyéb okból szükséges. Ha a bíróság által elektronikus úton megküldött bírósági irathoz e bekezdés szerinti melléklet kapcsolódik, a határidőt a melléklet átvételétől kell számítani.

(5) A bíróság felhívhatja a papír alapú kapcsolattartással eljáró szakértőt, illetve szakértői tevékenységet végző szervet, hogy a szakvéleményt adathordozón is nyújtsa be, ha azt elektronikus kapcsolattartással eljáró fél részére kell kézbesítenie. A szakértő, illetve a szakértői

tevékenységet végző szerv felel azért, hogy a papír alapú szakvélemény tartalma megegyező legyen az adathordozón benyújtott dokumentum tartalmával.

610. § *[A bíróságok egymás közötti és más szervekkel történő elektronikus kapcsolattartása]*

(1) A bíróság - a (2) bekezdésben foglalt kivétellel - másik bírósággal, valamint törvény alapján elektronikus ügyintézést biztosító szervvel, továbbá a Kormány által kijelölt közfeladatot ellátó szervvel a kapcsolatot elektronikus úton tartja.

(2) Az elektronikus kapcsolattartás alóli kivételt jelenti, ha a kézbesíttetni rendelt okirat papír alapú bemutatása, megtekintése szükséges; erre különösen akkor kerülhet sor, ha a papír alapú okirat valódisága vitás.

158. Az elektronikus kapcsolattartás eltérő szabályai

611. § *[A képviseletre vonatkozó szabályok elektronikus kapcsolattartás esetén]*

(1) A képviselő elektronikus kapcsolattartás esetén a keresetlevél vagy az első, a bírósághoz benyújtott beadvány mellékleteként csatolja az elektronikus okiratként rendelkezésre álló vagy az általa digitalizált meghatalmazást, kivéve, ha a képviselő meghatalmazása a rendelkezési nyilvántartásban a 67. § (3) bekezdésében foglaltaknak megfelelően szerepel. A bíróság - ha e tekintetben alapos kétsége merül fel - digitalizált meghatalmazás esetén az eredeti meghatalmazás bemutatására hívja fel a képviselőt az egyezőség megállapítása érdekében.

(2) A jogi képviselővel eljáró, de saját személyében elektronikus útra nem köteles fél a jogi képviselet visszavonására irányuló nyilatkozatát papír alapon is benyújthatja. A jogi képviselet visszavonásával egyidejűleg a fél nyilatkozik arról, hogy a nyilatkozat benyújtását követően jogi képviselő igénybevételével vagy jogi képviselő nélkül jár el.

(3) Ha a fél a jogi képviselet visszavonását követően jogi képviselővel jár el, a jogi képviselet visszavonásával egyidejűleg csatolja a nyilatkozat benyújtását követően eljáró új jogi képviselő meghatalmazását.

612. § [A beadványokra vonatkozó előírások elektronikus kapcsolattartás esetén]

Ha a perben a kapcsolattartás elektronikus úton történik, a határidő elmulasztásának következményeit - a napokban, munkanapokban, hónapokban vagy években megállapított határidő esetén - nem lehet alkalmazni, ha a bírósághoz intézett beadványt legkésőbb a határidő utolsó napján elektronikus úton az informatikai követelményeknek megfelelően előterjesztették.

613. § *[Papír alapú okiratok elektronikus kapcsolattartás esetén]*

(1) Az elektronikus úton történő kapcsolattartásra kötelezett és az elektronikus kapcsolattartást választó fél, illetve képviselő (a továbbiakban együtt: elektronikus úton kapcsolatot tartó) - ha a beadvány mellékletét képező okirat nem elektronikus okiratként áll rendelkezésre - köteles gondoskodni a beadvány mellékletét képező papír alapú okirat digitalizálásáról és a papír alapú okirat megőrzéséről.

(2) A papír alapú okirat - jogszabályban meghatározott módon történő - digitalizálására a bíróságnak öt munkanap áll rendelkezésére. Az irat digitalizálásához szükséges időt - legfeljebb azonban öt munkanapot - a határidő számítása szempontjából figyelmen kívül kell hagyni.

(3) Ha a fél az elektronikus úton történő kapcsolattartást választotta vagy elektronikus útra kötelezett, az elektronikus benyújtás alóli kivételt jelenti, ha az eljárásban az okirat papír alapú bemutatása, megtekintése szükséges; erre különösen akkor kerülhet sor, ha a papír alapú okirat valódisága vitás. A papír alapú benyújtást a bíróság hivatalból és a fél indítványára is elrendelheti.

(4) A bíróság az elektronikus úton benyújtott keresetlevél jogszabályban meghatározott módon készített papír alapú másolatát kézbesíti az alperes részére, ha az alperes elektronikus kapcsolattartásra nem köteles vagy az elektronikus kapcsolattartásra köteles alperes elektronikus kapcsolattartásra szolgáló elérhetősége nem ismert. A bíróság az alperest tájékoztatja arról, hogy ellenkérelmét, viszontkeresetét vagy egyéb beadványát elektronikus úton is benyújthatja vagy - ha arra köteles - elektronikus úton köteles benyújtani.

614. § *[Kézbesítés elektronikus kapcsolattartás esetén]*

(1) Ha a beadványt elektronikus úton nyújtják be, és az illetéket jogszabályban foglaltak szerint olyan módon kell megfizetni, amely alapján a bíróság az illeték megfizetéséről a keresetlevél benyújtásával egyidejűleg nem szerez tudomást, a 115. § (2) bekezdésében, a 176. § (1) bekezdés k) pontjában, valamint a 259. § (1) bekezdés a) pontjában foglaltak alkalmazásának a beadvány érkeztetését követő három munkanapon belül helye nincs.

(2) Ha az irat azért nem kézbesíthető, mert az elektronikus úton kapcsolatot tartó a kézbesítési rendszer azon szolgáltatása tekintetében nem kötött szolgáltatási szerződést vagy azt megszüntette, amelyen keresztül részére a bírósági iratokat kézbesíthetik, az elektronikus úton kapcsolatot tartót a bíróság pénzbírsággal sújtja és a bírósági iratot papír alapon kézbesíti.

(3) A beadvány elektronikus levélcímről történő benyújtása nem minősül elektronikus úton történő benyújtásnak, továbbá a bíróság csak e törvényben meghatározott esetben továbbíthat iratot a fél elektronikus levélcímére.

615. § *[Az Országos Bírósági Hivatal informatikai rendszere és az elektronikus kapcsolattartással összefüggő adatkezelés]*

(1) Az Országos Bírósági Hivatal az erre szolgáló informatikai rendszer alkalmazásával biztosítja, hogy a bírósággal kézbesítési szolgáltatást nyújtó rendszer útján folyamatosan lehessen kapcsolatot tartani.

(2) Az Országos Bírósági Hivatal és a bíróság jogosult az elektronikus úton kapcsolatot tartóknak az elektronikus kapcsolattartás biztosítása céljából hozzá érkezett adatainak kezelésére.

616. § *[Elektronikus bírósági irat]*

A bíróság az általa elektronikusan megküldött bírósági iratot a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendelet szerinti, törvényben vagy kormányrendeletben meghatározott feltételeknek megfelelő elektronikus bélyegzővel látja el. A bíróság által készített, törvényben vagy kormányrendeletben meghatározott feltételeknek megfelelő elektronikus bélyegzővel ellátott irat közokirat.

617. § *[A határidő számítása üzemzavar, üzemszünet esetén]*

A törvényi, illetve a bíróság által napokban és munkanapokban megállapított határidőbe nem számít bele az a nap - hónapokban és években megállapított határidő esetén az a lejárati nap -, amely során legalább négy órán át jogszabályban meghatározottak szerinti üzemzavar vagy üzemszünet állt fenn. Ha az órákban megállapított határidő jogszabályban meghatározott üzemzavar vagy üzemszünet fennállása alatt járna le, a határidő a következő munkanapon, a hivatali idő kezdetét követő első óra leteltével jár le.

618. § *[Az elektronikus kapcsolattartásra vonatkozó szabályok megszegésének következményei]*

(1) Ha az elektronikus úton kapcsolatot tartó beadványát

a) nem elektronikus úton, vagy
b) elektronikus úton, de nem az E-ügyintézési tv.-ben és végrehajtási rendeleteiben meghatározott módon

terjeszti elő - ha e törvény másként nem rendelkezik -, a bíróság a keresetlevelet, a bírósági meghagyással szembeni ellentmondást, a fellebbezést, a felülvizsgálati kérelmet és a perújítási kérelmet visszautasítja, az egyéb beadványban foglalt nyilatkozat pedig hatálytalan.

(2) Ha fizetési meghagyásos eljárás jogosultja e törvény alapján elektronikus úton kapcsolatot tartónak minősül és az ellentmondás előterjesztését követően a keresetet tartalmazó iratot a bíróság részére nem elektronikus úton terjeszti elő, a bíróság az eljárást hivatalból megszünteti.

(3) Az (1) bekezdés szerinti visszautasító végzés és a (2) bekezdés szerinti megszüntető végzés ellen külön fellebbezésnek van helye.

619. § *[Az elektronikus formátumban rendelkezésre álló irat továbbítása]*

(1) Az 50. alcímben foglalt jogosultságok gyakorlása érdekében a fél, az ügyész és a perben részt vevő egyéb személy, valamint azok képviselője írásban vagy a tárgyaláson kérheti, hogy a részére kiadható iratot elektronikus formában az általa megjelölt elektronikus levélcímre továbbítsa a bíróság, ha az irat

a) elektronikus formában,
b) elektronikus okiratként vagy

c) a papíralapú okirat elektronikus másolataként

a bíróságnál rendelkezésre áll.

(2) Az (1) bekezdésben meghatározott esetben az irat továbbításáért nem kell illetéket fizetni. Az irat akkor áll elektronikus formában rendelkezésre, ha a bíróság a papír alapú iratot informatikai eszköz alkalmazásával szerkesztette meg; az elektronikus formában rendelkezésre álló irat nem hiteles kiadmány, az bizonyítékként nem használható fel.

620. § *[Iratbetekintés elektronikus hozzáférés biztosítása útján]*

Az 50. alcímben foglalt jogosultságok gyakorlása érdekében a bíróság az iratbetekintésre jogosultak számára a per irataihoz történő elektronikus hozzáférés lehetőségét jogszabály rendelkezései alapján biztosítja.

621. § [*A hangkapcsolatot biztosító elektronikus úton megtett nyilatkozat joghatása]*

Kizárólag hangkapcsolatot biztosító elektronikus úton nyilatkozat nem tehető; az ilyen módon tett nyilatkozat hatálytalan.

2017. évi I. törvény a közigazgatási perrendtartásról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=200732.338649

29. § *[Elektronikus technológiák és eszközök alkalmazása]*

(1) Az elektronikus kapcsolattartásra a polgári perrendtartás szabályait kell megfelelően alkalmazni.

36. § *[A polgári perrendtartás egyéb általános szabályainak alkalmazása]*

(1) A polgári perrendtartás szabályait kell alkalmazni

a) a nyelvhasználatra,
b) a bíróság általános intézkedési és tájékoztatási kötelezettségére,
c) a kézbesítésre,
d) az idézésre,
e) a határidőre,
f) az ítélkezési szünetre,
g) a mulasztásra és annak igazolására,
h) az eljárás anyagának rögzítésére,
i) az iratok megtekintésére, a másolatkészítésre és az adatkezelésre,

2016. évi CL. törvény az általános közigazgatási rendtartásról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=199170.338647

12. A kapcsolattartás általános szabályai

26. § *[A kapcsolattartás általános szabályai]*

(1) A hatóság írásban, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvényben (a továbbiakban: Eüsztv.) meghatározott elektronikus úton (a továbbiakban együtt: írásban), vagy személyesen, írásbelinek nem minősülő elektronikus úton (a továbbiakban együtt: szóban) tart kapcsolatot az ügyféllel és az eljárásban résztvevőkkel.

(2) Ha törvény másként nem rendelkezik, a kapcsolattartás formáját a hatóság tájékoztatása alapján az ügyfél választja meg. Az ügyfél a választott kapcsolattartási módról más - a hatóságnál rendelkezésre álló - módra áttérhet.

(3) Életveszéllyel vagy súlyos kárral fenyegető helyzet esetén a hatóság választja meg a kapcsolattartás módját.

13. Adatkezelés

27. § *[Az adatkezelés szabályai]*

(1) A hatóság jogosult az ügyfél és az eljárás egyéb résztvevője természetes személyazonosító adatainak és az ügyfajtát szabályozó törvényben meghatározott személyes adatok, továbbá - ha törvény másként nem rendelkezik - a tényállás tisztázásához elengedhetetlenül szükséges más személyes adatok megismerésére és kezelésére. A kérelemre induló eljárásban vélelmezni kell, hogy a kérelmező ügyfél a tényállás tisztázásához szükséges személyes adatok - ideértve a különleges adatokat is - kezeléséhez hozzájárulást adott.

(2) A hatóság gondoskodik arról, hogy a törvény által védett titok (a továbbiakban: védett adat) ne kerüljön nyilvánosságra, ne juthasson illetéktelen személy tudomására, és a személyes adatok védelme biztosított legyen.

(3) A hatóság az eljárása során annak lefolytatásához - jogszabályban meghatározott módon és körben - megismerheti azokat a védett adatokat, amelyek eljárásával összefüggnek, illetve amelyek kezelése az eljárás eredményes lefolytatása érdekében szükséges.

14. Adatok zárt kezelése

28. § *[Az adatok zárt kezelése]*

(1) Indokolt esetben a hatóság kérelemre vagy hivatalból elrendeli az ügyfél és az eljárás egyéb résztvevője természetes személyazonosító adatainak és lakcímének zárt kezelését, ha az

eljárásban való közreműködése miatt súlyosan hátrányos következmény érheti. A végzést a kérelmet előterjesztővel kell közölni.

(2) A szakértő az (1) bekezdésben foglaltak szerint az igazságügyi szakértői névjegyzék nyilvános adatain kívüli természetes személyazonosító adatai és lakcíme zárt kezelését kérheti.

(3) A természetes személyazonosító adatokat és a lakcímet a hatóság az ügy iratai között elkülönítve, zártan kezeli és biztosítja, hogy a zártan kezelt adatok az eljárási cselekmények során ne váljanak megismerhetővé.

46. A döntés közlése

85. § *[A döntés közlésének általános szabályai]*

(1) A határozatot a hatóság közli az ügyféllel, azzal, akire nézve az rendelkezést tartalmaz, az ügyben eljárt szakhatósággal.

(2) A végzést a hatóság közli azzal, akire nézve az rendelkezést tartalmaz, és akinek a jogát vagy jogos érdekét érinti. A hatóság az ügyfél kérelmére egy ízben, külön illeték vagy díj felszámítása nélkül ad ki másolatot a vele nem közölt végzésről.

(3) A hatóság a döntést írásbeli kapcsolattartás esetén hivatalos iratként vagy az Eüsztv.-ben meghatározott elektronikus úton kézbesíti.

(4) Ha jogszabály nem zárja ki, a döntést szóban is közölni lehet az (1) és (2) bekezdésben meghatározott személlyel. A közlés tényét és időpontját az iratra fel kell jegyezni, és azt alá kell íratni. Ha azt az (1) és (2) bekezdésben meghatározott személy kéri, a szóban közölt döntést a hatóság írásban is megküldi a részére.

(5) Ha törvény vagy kormányrendelet másként nem rendelkezik, a döntés közlésének napja

a) az a nap, amelyen azt írásban vagy szóban közölték, vagy
b) a hirdetmény kifüggesztését követő tizenötödik nap.

(6) Ha a hatóság életveszéllyel vagy súlyos kárral fenyegető helyzetben, valamint törvény rendelkezése alapján a döntést nem az e törvényben meghatározott feltételeknek megfelelő módon közli, a döntést írásban is megküldi. A döntés közlésének napja ilyenkor - kizárólag a jogorvoslati határidők számításának szempontjából - az írásbeli közlés napja.

86. § *[A kézbesítésre vonatkozó szabályok]*

(1) A nem elektronikusan közölt iratot a kézbesítés megkísérlésének napján kézbesítettnek kell tekinteni, ha a címzett az átvételt megtagadta. Ha a kézbesítés azért volt sikertelen, mert az a címzett hatósági nyilvántartásban szereplő lakcíméről vagy székhelyéről a hatósághoz

a) „nem kereste” jelzéssel érkezett vissza, az iratot a kézbesítés második megkísérlésének napját,
b) „ismeretlen” vagy „elköltözött” jelzéssel érkezett vissza, az iratot a kézbesítés

megkísérlésének napját

követő ötödik munkanapon kézbesítettnek kell tekinteni.

(2) Ha a címzett tudomást szerez arról, hogy a neki küldött iratot a hatóság kézbesítettnek tekinti, a tudomásszerzéstől számított tizenöt napon belül, de legkésőbb a közléstől számított negyvenöt napon belül kifogást terjeszthet elő.

(3) A kifogásnak a hatóság akkor ad helyt, ha a címzett az iratot azért nem vehette át, mert

a) a kézbesítés a hivatalos iratok kézbesítésére vonatkozó jogszabályok megsértésével történt, vagy más okból nem volt szabályszerű, vagy

b) az iratot más, az *a)* pontban nem említett önhibáján kívüli okból nem volt módja átvenni.

(4) Nem természetes személy címzett csak akkor terjeszthet elő kifogást, ha a kézbesítés nem szabályszerűen történt.

(5) A kifogásban elő kell adni azokat a tényeket, illetve körülményeket, amelyek a kézbesítés szabálytalanságát igazolják vagy az önhiba hiányát valószínűsítik. Ha a kifogásnak a hatóság helyt ad, az igazolási kérelemre vonatkozó szabályokat kell alkalmazni.

(6) A kifogást az a hatóság bírálja el, amelyik a kézbesítés tárgyát képező iratot kiadmányozta.

(7) A hatósági kézbesítő általi kézbesítésre az e §-ban foglalt rendelkezéseket kell alkalmazni.

87. § *[A kézbesítési meghatalmazottra vonatkozó szabályok]*

(1) Az ügyfél köteles az első kapcsolatfelvétel alkalmával - a kézbesítési meghatalmazás előterjesztésével együtt - kézbesítési meghatalmazottat megnevezni, ha

a) magyarországi lakcímmel vagy székhellyel nem rendelkezik,

b) képviselőt nem nevezett meg, és

c) elektronikus kapcsolattartásnak nincs helye.

(2) A kézbesítési meghatalmazott az eljárásban keletkezett, az ügyféllel közlendő döntéseket és iratokat átveszi, és azokat az ügyfél részére továbbítja.

(3) Az ügyfél részére szóló és a kézbesítési meghatalmazottal szabályszerűen közölt döntést úgy kell tekinteni, hogy az a meghatalmazottal történt közlést követő tizenötödik napon minősül az ügyféllel közöltnek.

(4) Ha hirdetményi közlésnek lenne helye, és a döntés az ügyfél számára kötelezettséget állapít meg, vagy alapvető jogát vonja el vagy korlátozza, a döntés közlésének megkísérlése érdekében kézbesítési ügygondnok rendelhető ki, aki gondoskodik az ügyfél tartózkodási helyének megállapításáról és a döntés kézbesítéséről.

(5) Ha a kézbesítési ügygondnok nem járt sikerrel, a döntést azon a napon kell kézbesítettnek tekinteni, amikor a kézbesítés sikertelenségét a kézbesítési ügygondnok az őt kirendelő hatóságnak bejelenti, de legkésőbb a kirendeléstől számított tizenötödik napon.

(6) Sikeres kézbesítés esetén a kézbesítési ügygondnok a sikeres kézbesítés napjáról és az ügyfél tartózkodási helyéről haladéktalanul értesíti az őt kirendelő hatóságot.

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

http://njt.hu/cgi_bin/njt_doc.cgi?docid=57566.338462

1. § (1) E törvény rendelkezéseit kell alkalmazni:

a) a Magyarország területéről nyújtott, valamint a Magyarország területére irányuló információs társadalommal összefüggő szolgáltatásra;

b) az a) pontban meghatározott szolgáltatás tekintetében igénybe vevőnek, illetve szolgáltatónak minősülő természetes, illetve jogi személyre vagy jogi személyiség nélküli szervezetre.

(3) E törvény hatálya nem terjed ki a bírósági, illetőleg egyéb hatósági eljárásban nyújtott és felhasznált információs társadalommal összefüggő szolgáltatásra és nem érinti a személyes adatok védelmére vonatkozó jogszabályok alkalmazását.

(4) E törvény hatálya - a 2. § *m)* pont, 3/B. §, 4/A. § valamint 13/B. § kivételével - nem terjed ki az olyan közlésekre, amelyet gazdasági vagy szakmai tevékenység, vagy közfeladat körén kívül eső célból eljáró személy tesz információs társadalommal összefüggő szolgáltatás igénybevételével, ideértve az ilyen módon tett szerződéses nyilatkozatokat is.

Értelmező rendelkezések

2. § E törvény alkalmazásában:

a) *Elektronikus kereskedelmi szolgáltatás:* olyan információs társadalommal összefüggő szolgáltatás, amelynek célja valamely birtokba vehető forgalomképes ingó dolog - ideértve a pénzt és az értékpapírt, valamint a dolog módjára hasznosítható természeti erőket -, szolgáltatás, ingatlan, vagyoni értékű jog (a továbbiakban együtt: áru) üzletszerű értékesítése, beszerzése, cseréje vagy más módon történő igénybevétele;

b) *Elektronikus út:* elektronikus adatfeldolgozást, -tárolást, illetőleg -továbbítást végző vezetékes, rádiótechnikai, optikai vagy más elektromágneses eszközök alkalmazása;

d) *Igénybe vevő:* az a természetes, illetve jogi személy vagy jogi személyiség nélküli szervezet, aki/amely információs társadalommal összefüggő szolgáltatást vesz igénybe;

e) *Információ:* bármely, elektronikus úton feldolgozható, tárolható, továbbítható adat, jel, kép tekintet nélkül arra, hogy annak tartalma jogi védelemben részesül-e;

f) *Információs társadalommal összefüggő szolgáltatás:* elektronikus úton, távollevők részére, rendszerint ellenszolgáltatás fejében nyújtott szolgáltatás, amelyhez a szolgáltatás igénybe vevője egyedileg fér hozzá;

g) *Magyarország területére irányuló szolgáltatás:* minden olyan szolgáltatás, melyről a használt nyelv, a pénznem és egyéb körülmények alapján valószínűsíthető, hogy magyarországi igénybe vevők számára kívánják elérhetővé tenni; továbbá az m) pont szerinti alkalmazásszolgáltató valamennyi olyan információs társadalommal összefüggő szolgáltatása, amely Magyarországon elérhető, függetlenül attól, hogy az alkalmazásszolgáltató Magyarországon letelepedett, vagy bármilyen formában engedélyezett-e, vagy attól, hogy a hozzáférés során akár a szolgáltató, akár a felhasználó egyértelműen azonosítható-e;;

h) *Magyarország területéről nyújtott szolgáltatás*: Magyarország területén lévő székhelyén, telephelyén vagy lakóhelyén az adott információs társadalommal összefüggő szolgáltatással kapcsolatos tényleges tevékenységet végző szolgáltató által nyújtott információs társadalommal összefüggő szolgáltatás;

k) *Szolgáltató:* az információs társadalommal összefüggő szolgáltatást nyújtó természetes, illetve jogi személy vagy jogi személyiség nélküli szervezet;

l) *Közvetítő szolgáltató:* az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely

la) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);

lb) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);

lc) az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);

ld) információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás);

le) alkalmazásszolgáltató

v) *Fogyasztó:* a önálló foglalkozásán és gazdasági tevékenységén kívül eső célok érdekében eljáró természetes személy.

Az előzetes engedélyezést kizáró elv

3. § (1) Információs társadalommal összefüggő szolgáltatás nyújtásának megkezdéséhez, illetve folytatásához előzetes engedély vagy bármely ezzel azonos joghatású hatósági határozat nem szükséges.

(2) Az (1) bekezdés nem érinti

a) az információs társadalommal összefüggő szolgáltatás útján végzett tevékenységre külön jogszabályban, nem az elektronikus úton történő szolgáltatásnyújtásra tekintettel előírt minősítési, képesítési, engedélyezési vagy bejelentési kötelezettséget; valamint

b) az elektronikus hírközlésről szóló törvényben, illetve a törvény felhatalmazása alapján megalkotott jogszabályban előírt engedélyezési, illetve bejelentési kötelezettséget.

3/A. § (1) Az Európai Gazdasági Térségről szóló megállapodás más részes államai területén letelepedett szolgáltató által a Magyarország területére irányuló szolgáltatás nem korlátozható, kivéve, ha az érintett hatóság vagy bíróság intézkedése

a) az alábbi érdekek valamelyikének védelmében szükséges:
  aa) a közrend, különösen a bűncselekmények megelőzése, nyomozása, felderítése és üldözése, ideértve a kiskorúak védelmét és a faji, nemi, vallási vagy nemzeti alapú bármilyen gyűlöletre uszítás és az egyének emberi méltóságának megsértése elleni fellépést,
  ab) a közegészség,
  ac) a közbiztonság, ideértve a nemzetbiztonsági és honvédelmi érdekeket is,
  ad) a fogyasztók vagy a befektetők érdekei; és
b) olyan, adott információs társadalommal összefüggő szolgáltatás ellen irányul, amely az *a)* pontban említett érdekeket sérti vagy súlyosan veszélyezteti; és
c) az érdeksérelemmel, illetve a veszélyeztetéssel arányos.

(2) Az érintett hatóság az intézkedés megtételét megelőzően köteles tájékoztatni az Európai Bizottságot, valamint megkereséssel fordul az Európai Gazdasági Térségről szóló megállapodás érintett részes államának hatáskörrel rendelkező hatóságához az érintett államban letelepedett szolgáltatóval szembeni intézkedés végett. Amennyiben az Európai Bizottság nem tesz ellenvetést, továbbá a megkeresett tagállami hatóság nem intézkedik időben vagy nem megfelelő intézkedést tesz, a hatóság végrehajtja az intézkedést.

Az információs társadalommal összefüggő szolgáltatással kapcsolatos adatszolgáltatás

4. § A szolgáltató köteles elektronikus úton közvetlenül és folyamatosan, könnyen hozzáférhető módon legalább a következő adatokat közzétenni:

a) a szolgáltató nevét,
b) a szolgáltató székhelyét, telephelyét, ennek hiányában lakcímét,
c) a szolgáltató elérhetőségére vonatkozó adatokat, különösen az igénybe vevőkkel való kapcsolattartásra szolgáló, rendszeresen használt elektronikus levelezési címét,
d) ha a szolgáltató létrejöttét vagy tevékenysége gyakorlásának megkezdését jogszabály nyilvántartásba való bejegyzéshez köti, a szolgáltatót a nyilvántartásba bejegyző bíróság vagy hatóság megnevezését, és a szolgáltató nyilvántartásba vételi számát,
e) ha a szolgáltató tevékenységének gyakorlása jogszabály alapján engedélyköteles, ezt a tényt az engedélyező hatóság megnevezésével és elérhetőségi adataival, valamint az engedély számával együtt,
f) ha a szolgáltató az általános forgalmi adó alanya, a szolgáltató adószámát;
g) a szabályozott szakmák gyakorlásának körében:
  ga) annak a szakmai érdek-képviseleti szervnek (kamarának) a megnevezését, amelynek a szolgáltató akár kötelező előírás alapján, akár önkéntesen tagja;

gb) a természetes személy szolgáltató szakképzettségének, illetve szakmai, tudományos fokozatának, valamint annak a tagállamnak a megjelölését, ahol ezt a szakképzettséget, illetve fokozatot megszerezte;

gc) hivatkozást a szabályozott szakma gyakorlásának a szolgáltató letelepedési helye szerinti államban alkalmazandó szakmai szabályaira, és az azokhoz való hozzáférés módjára.

Az elektronikus úton történő szerződéskötésre vonatkozó szabályok

5. § (1) A szolgáltató köteles az információs társadalommal összefüggő szolgáltatásra vonatkozó általános szerződési feltételeket oly módon hozzáférhetővé tenni, amely lehetővé teszi az igénybe vevő számára, hogy tárolja és előhívja azokat.

(2) A szolgáltató az igénybe vevő megrendelésének elküldését megelőzően köteles egyértelműen tájékoztatni az igénybe vevőt:

a) azokról a technikai lépésekről, amelyeket a szerződés elektronikus úton való megkötéséhez meg kell tenni;

b) arról, hogy a megkötendő szerződés írásba foglalt szerződésnek minősül-e, a szolgáltató iktatja-e a szerződést, illetve, hogy az iktatott szerződés utóbb hozzáférhető lesz-e;

c) az adatbeviteli hibáknak a szerződéses nyilatkozat elküldését megelőzően történő azonosításához és kijavításához biztosított eszközökről;

d) a szerződéskötés lehetséges nyelveiről;

e) arról a - szolgáltatási tevékenységére vonatkozó - magatartási kódexről, amelynek az adott szolgáltatás tekintetében aláveti magát, amennyiben van ilyen; továbbá arról, hogy ez a magatartási kódex elektronikus úton hol hozzáférhető.

(3) A szolgáltató és a fogyasztónak nem minősülő igénybe vevő közötti szerződéskötés során a felek kölcsönös megállapodással eltérhetnek a (2) bekezdés rendelkezéseitől.

(4) Nem kell alkalmazni e § rendelkezéseit a kizárólag elektronikus levelezés vagy azzal egyenértékű egyéni kommunikációs eszközzel tett címzett nyilatkozatok útján történő szerződéskötésre.

6. § (1) A szolgáltató köteles megfelelő, hatékony és hozzáférhető technikai eszközökkel biztosítani, hogy az igénybe vevő az adatbeviteli hibák azonosítását és kijavítását megrendelésének elektronikus úton való elküldése előtt el tudja végezni. Ilyen lehetőség hiányában az igénybe vevő megrendelése nem minősül szerződéses nyilatkozatnak.

(2) A szolgáltató köteles az igénybe vevő megrendelésének megérkezését az igénybe vevő felé elektronikus úton haladéktalanul visszaigazolni. Amennyiben e visszaigazolás az igénybe vevő megrendelésének elküldésétől számított, a szolgáltatás jellegétől függő elvárható határidőn belül, de legkésőbb 48 órán belül az igénybe vevőhöz nem érkezik meg, az igénybe vevő mentesül az ajánlati kötöttség vagy szerződéses kötelezettség alól.

(3) A megrendelés és annak visszaigazolása akkor tekintendő a szolgáltatóhoz, illetve az igénybe vevőhöz megérkezettnek, amikor az számára hozzáférhetővé válik.

(4) A szolgáltató és a fogyasztónak nem minősülő igénybe vevő közötti szerződéskötés során a felek eltérhetnek az (1)-(2) bekezdés rendelkezéseitől, ha erről megállapodtak.

(5) Az (1) és (2) bekezdések rendelkezéseit nem kell alkalmazni a kizárólag elektronikus levelezés vagy azzal egyenértékű egyéni kommunikációs eszközzel tett címzett nyilatkozatok útján történő szerződéskötésre.

A szolgáltató és a közvetítő szolgáltató felelőssége

7. § (1) A szolgáltató felel az általa rendelkezésre bocsátott, jogszabályba ütköző tartalmú információért.

(2) A közvetítő szolgáltató a más által rendelkezésre bocsátott, a közvetítő szolgáltató által nyújtott információs társadalommal összefüggő szolgáltatással továbbított, tárolt vagy hozzáférhetővé tett információért - a 8-11. §-okban meghatározott feltételek fennállása esetén - nem felel.

(3) A közvetítő szolgáltató nem köteles ellenőrizni az általa csak továbbított, tárolt, hozzáférhetővé tett információt, továbbá nem köteles olyan tényeket vagy körülményeket keresni, amelyek jogellenes tevékenység folytatására utalnak.

(4) A 13. § (1) bekezdése szerinti jogsértés esetében a 2. § *lb)-ld)* pontjaiban meghatározott közvetítő szolgáltató - a (2) bekezdésben említetteken túlmenően - akkor nem felel a más által rendelkezésre bocsátott, az általa nyújtott információs társadalommal összefüggő szolgáltatással továbbított, tárolt vagy hozzáférhetővé tett jogszabályba ütköző tartalmú információval harmadik személynek okozott jogsérelemért, ha lefolytatja a 13. § szerinti eljárást.

(5) A közvetítő szolgáltatónak a (2) bekezdés alapján történő mentesülése nem zárja ki azt, hogy az a személy, akit a jogellenes tartalmú információ révén sérelem ért, a jogsértésből fakadó igényei közül a jogsértés megelőzésére vagy abbahagyására irányuló követeléseit a jogsértő fél mellett a közvetítő szolgáltatóval szemben is bíróság útján érvényesítse.

(6) A közvetítő szolgáltató nem felel az információ eltávolítása vagy hozzáférés nem biztosítása révén keletkezett jogsérelemért, amennyiben a 7-11. § vagy a 13. § szerint járt el.

8. § (1) A 2. § *l)* pont *la)* alpontjában, valamint *m)* pontjában meghatározott közvetítő szolgáltató akkor nem felel a továbbított információért, ha

a) nem a szolgáltató kezdeményezi az információ továbbítását;
b) nem a szolgáltató választja meg a továbbítás címzettjét, és
c) a továbbított információt nem a szolgáltató választja ki, illetve azt nem változtatja meg.

(2) Az információtovábbítás és a hozzáférés (1) bekezdés szerinti lehetővé tétele magában foglalja a továbbított információ közbenső és átmeneti jellegű automatikus tárolását is,

amennyiben ez kizárólag az információtovábbítás lebonyolítására szolgál és az információt nem tárolják hosszabb ideig, mint az a továbbításhoz szükséges.

9. § A 2. § *lb)* pontjában meghatározott közvetítő szolgáltató akkor nem felel az információ közbenső és átmeneti jellegű automatikus tárolásával okozott kárért, ha

a) a szolgáltató nem változtatja meg az információt;
b) a tárolt információhoz való hozzáférés megfelel az információ hozzáférésével kapcsolatban támasztott feltételeknek;
c) a közbenső tárolóban az információ frissítése megfelel a széleskörűen elismert és alkalmazott információfrissítési gyakorlatnak;
d) a közbenső tárolás nem zavarja meg az információ felhasználásával kapcsolatos adatok kinyerésére szolgáló, széleskörűen elismert és alkalmazott technológia jogszerű használatát; és
e) a szolgáltató haladéktalanul eltávolítja az általa tárolt információt vagy nem biztosítja az ahhoz való hozzáférést, amint tudomást szerzett arról, hogy az információt az adatátvitel eredeti kiindulási pontján a hálózatról eltávolították, vagy az ahhoz való hozzáférés biztosítását megszüntették, illetve, hogy a bíróság vagy más hatóság az eltávolítást vagy a hozzáférés megtiltását elrendelte.

10. § A 2. § *lc)* pontjában meghatározott közvetítő szolgáltató akkor nem felel az igénybe vevő által biztosított információért, ha

a) nincs tudomása az információval kapcsolatos jogellenes magatartásról, vagy arról, hogy az információ bárkinek a jogát vagy jogos érdekét sérti;
b) amint az *a)* pontban foglaltakról tudomást szerzett, haladéktalanul intézkedik az információ eltávolításáról, vagy a hozzáférést nem biztosítja.

11. § A 2. § *ld)* pontjában meghatározott közvetítő szolgáltató akkor nem felel az információ 2. § *ld)* pontja szerinti hozzáférhetővé tételével okozott kárért, ha

a) nincs tudomása az információval kapcsolatos jogellenes magatartásról, vagy arról, hogy az információ bárkinek a jogát vagy jogos érdekét sérti;
b) amint az *a)* pontban foglaltakról tudomást szerzett, haladéktalanul intézkedik az elérési információ eltávolításáról vagy a hozzáférés megtiltásáról.

12. § A 10-11. §-ok rendelkezései alapján a szolgáltató nem mentesül a felelősség alól, ha az igénybe vevő a szolgáltató megbízásából vagy utasításai alapján cselekszik.

Adatvédelem

13/A. § (1) A szolgáltató az információs társadalommal összefüggő szolgáltatás nyújtására irányuló szerződés létrehozása, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, az abból származó díjak számlázása, valamint az azzal kapcsolatos

követelések érvényesítése céljából kezelheti az igénybe vevő azonosításához szükséges természetes személyazonosító adatokat és lakcímet.

(2) A szolgáltató az információs társadalommal összefüggő szolgáltatás nyújtására irányuló szerződésből származó díjak számlázása céljából kezelheti az információs társadalommal összefüggő szolgáltatás igénybevételével kapcsolatos természetes személyazonosító adatokat,

lakcímet, valamint a szolgáltatás igénybevételének időpontjára, időtartamára és helyére vonatkozó adatokat.

(3) A szolgáltató - a (2) bekezdésben foglaltakon túlmenően - a szolgáltatás nyújtása céljából kezelheti azon személyes adatokat, amelyek a szolgáltatás nyújtásához technikailag elengedhetetlenül szükségesek. A szolgáltatónak az egyéb feltételek azonossága esetén úgy kell megválasztania és minden esetben oly módon kell üzemeltetnie az információs társadalommal összefüggő szolgáltatás nyújtása során alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez feltétlenül szükséges, azonban ebben az esetben is csak a szükséges mértékben és ideig.

(4) A szolgáltató a szolgáltatás igénybevételével kapcsolatos adatokat bármely, a (3) bekezdésben meghatározottaktól eltérő célból - így különösen szolgáltatása hatékonyságának növelése, az igénybe vevőnek címzett elektronikus hirdetés vagy egyéb címzett tartalom eljuttatása, piackutatás céljából - csak az adatkezelési cél előzetes meghatározása mellett és az igénybe vevő hozzájárulása alapján kezelhet.

(5) Az igénybe vevőnek az információs társadalommal összefüggő szolgáltatás igénybevételét megelőzően és a szolgáltatás igénybevétele során is folyamatosan biztosítani kell, hogy a (4) bekezdés szerinti adatkezelést megtilthassa.

(6) A (4) bekezdésben meghatározott adatok nem kapcsolhatók össze az igénybe vevő azonosító adataival és az igénybe vevő hozzájárulása nélkül nem adhatók át harmadik személy számára.

(7) Az (1)-(3) bekezdésben meghatározott célokból kezelt adatokat törölni kell a szerződés létrejöttének elmaradását, a szerződés megszűnését, valamint a számlázást követően. A (4) bekezdésben meghatározott célból kezelt adatokat törölni kell, ha az adatkezelési cél megszűnt, vagy az igénybe vevő így rendelkezik. Törvény eltérő rendelkezése hiányában az adattörlést haladéktalanul el kell végezni.

(8) Az információs társadalommal összefüggő szolgáltatás nyújtása nem tehető függővé az igénybe vevőnek valamely (1)-(3) bekezdésében nem említett célból történő adatkezeléshez való hozzájárulásától, amennyiben az adott szolgáltatás más szolgáltatótól nem vehető igénybe.

13/B. § (1) Az az alkalmazásszolgáltató, aki titkosított kommunikációt biztosító szolgáltatást nyújt, köteles az ilyen alkalmazás igénybevételével továbbított küldeményekkel, közlésekkel

kapcsolatosan keletkező vagy kezelt, (2) bekezdés szerinti metaadatokat azok keletkezésétől számított 1 évig megőrizni.

(2) A külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén a titkosított kommunikációt biztosító szolgáltatást nyújtó alkalmazásszolgáltató

a) a szolgáltatás típusát;
b) a szolgáltatás előfizetőjének vagy felhasználójának
  ba) a szolgáltatás igénybevételéhez szükséges azonosító adatait, a szolgáltatás igénybevételének dátumát, kezdő és záró időpontját;
  bb) a regisztrációhoz használt IP-címét és portszámát;
  bc) az igénybevételnél használt IP-címét és portszámát;
c) a felhasználói azonosítót

köteles átadni.

1998. évi XIX. törvény a büntetőeljárásról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=34361.328856

A kézbesítés

70. § (1) A bíróság, az ügyész, illetőleg a nyomozó hatóság hivatalos iratának az érintett személy részére átadása (kézbesítés) történhet

a) személyesen,
b) posta útján,
c) hirdetményi úton,
d) a bíróság, az ügyész, illetőleg a nyomozó hatóság kézbesítője útján,
e) nemzetközi jogsegély keretében,
f) elektronikus úton az E-ügyintézési törvény szerinti hivatalos elérhetőségre, illetve biztonságos elektronikus kapcsolattartásra szolgáló elérhetőségre.

(2) A címzett az iratot az azt küldőnél is átveheti.

(3) Ha a sértettnek vagy az egyéb érdekeltnek kézbesítési megbízottja van, a részükre szóló iratot - az idézés kivételével - a megbízottnak kell kézbesíteni.

(3a) Ha a címzett rendelkezik értesítési címmel, és a kézbesítést erre a címre kéri, a részére szóló iratot az értesítési címre kell kézbesíteni.

(4) A kézbesítés szabályszerű, ha a hivatalos iratot a címzett vagy helyette a külön jogszabály szerint átvételre jogosult más személy átvette. A hivatalos iratot szabályszerűen kézbesítettnek kell tekinteni, ha az irat átvételét, illetőleg a kézbesítési bizonyítvány (tértivevény) aláírását megtagadják.

(5) Hirdetményi úton kell kézbesíteni

a) a hivatalos iratot az ismeretlen helyen tartózkodó terhelt részére, és

b) az értesítést, ha ezt az érdekeltek jelentős száma indokolttá teszi.

(5a) Hirdetményi kézbesítés esetén a hirdetmény tartalmazza, hogy a címzett az iratot melyik bíróságnál, ügyészségnél, illetve nyomozó hatóságnál veheti át. Hirdetményben az értesítettek neve nem közölhető.

(6) A hirdetményt tizenöt napra közzé kell tenni a kézbesítést elrendelő bíróság, ügyészség vagy nyomozó hatóság elektronikus tájékoztatásra szolgáló honlapján, és tizenöt napra ki kell függeszteni a bíróság, ügyészség vagy nyomozó hatóság hirdetőtáblájára.

(6a) Az (5) bekezdés *a)* pontja esetén a hirdetményt tizenöt napra a terhelt utolsó ismert belföldi lakóhelye vagy tartózkodási helye szerinti helyi önkormányzat hirdetőtáblájára is ki kell függeszteni.

(6b) Az iratot a hirdetménynek a kézbesítést elrendelő bíróság, ügyészség vagy nyomozó hatóság hirdetőtábláján történt kifüggesztésétől számított tizenötödik napon kell kézbesítettnek tekinteni.

(7) A kézbesítési bizonyítvánnyal (tértivevénnyel) feladott hivatalos iratot a kézbesítés második megkísérlésének napját követő ötödik munkanapon kézbesítettnek kell tekinteni, ha a kézbesítés azért volt eredménytelen, mert a címzett az iratot nem vette át.

(8) A katonának [Btk. 127. § (1) bekezdés] kézbesítendő iratot az elöljárója útján kell kézbesíteni. A kézbesítés az elöljáró egyidejű értesítése mellett közvetlenül is történhet, ha a katonának az iratot küldő bíróság, ügyész vagy nyomozó hatóság székhelyén nincs elöljárója, és a késedelmes kézbesítés az eljárás sikerét vagy a katona jogát vagy méltányolható érdekét sértené. Ha a katona szolgálati viszonya a büntetőeljárás alatt megszűnik, a kézbesítésre az általános szabályok az irányadók.

(9) Ha a címzett fogva van, a neki kézbesítendő iratot - idézés és értesítés esetén az intézetnek szóló, az előállításra vonatkozó megkereséssel egyidejűleg - a fogvatartást végrehajtó intézet parancsnoka útján kell kézbesíteni.

70/A. § (1) A 70. § (7) bekezdésében meghatározott kézbesítési vélelem megdöntése iránt a címzett terjeszthet elő kérelmet, ha

a) a kézbesítés a hivatalos iratok kézbesítésére vonatkozó jogszabályok megsértésével történt, vagy

b) a hivatalos iratot nem az *a)* pontban meghatározott okból, önhibáján kívül nem vette át.

(2) A kérelemben elő kell adni azokat a tényeket, illetve körülményeket, amelyek a kézbesítés szabálytalanságát igazolják, vagy az (1) bekezdés *b)* pontjában meghatározott esetben a címzett részéről az önhiba hiányát valószínűsítik.

(3) A kézbesítési vélelem megdöntése iránti kérelemről az a bíróság, ügyész, illetőleg nyomozó hatóság határoz, amelynek eljárása során a kézbesítés történt. A kérelem előterjesztésére és elbírálására a mulasztás igazolására vonatkozó rendelkezéseket (65. és 66. §) kell megfelelően alkalmazni azzal, hogy a kérelem előterjesztésével együtt nem kell pótolni az elmulasztott cselekményt.

(4) Ha a kézbesítési vélelem megdöntése iránt a terhelt, a védő, a magánvádló vagy a pótmagánvádló terjeszt elő kérelmet, és a bíróság, ügyész, illetőleg nyomozó hatóság a kérelemnek helyt ad, a vélelmezett kézbesítéshez fűződő jogkövetkezmények hatálytalanok, és a kézbesítést, illetve a már megtett intézkedéseket, eljárási cselekményeket a szükséges mértékben meg kell ismételni. A megismétlés eredményéhez képest a korábbi eljárási cselekmények hatályban tartásáról vagy teljes, illetőleg részleges hatályon kívül helyezéséről is határozni kell.

(5) A (4) bekezdésben fel nem sorolt címzett által benyújtott kérelem esetében, ha a bíróság, ügyész, illetőleg nyomozó hatóság a kérelemnek helyt ad, a címzett vonatkozásában érvényesülő, a kézbesítéshez fűződő jogkövetkezmények nem alkalmazhatók, és a kézbesítést meg kell ismételni.

Másolat készítése az eljárás során keletkezett iratról

70/B. § (1) Az eljárás során keletkezett iratról - ideértve a bíróság, az ügyész és a nyomozó hatóság által beszerzett, illetőleg a büntetőeljárásban részt vevő személyek által benyújtott, valamint csatolt iratot is - az a bíróság, ügyész, illetőleg nyomozó hatóság, amely előtt az eljárás folyamatban van, a büntetőeljárásban részt vevő személyek kérelmére a (2)-(7) bekezdés szerint legkésőbb a kérelem előterjesztésétől számított nyolc napon belül másolatot ad ki.

(2) A nyomozás befejezéséig a gyanúsított, a védő, a fiatalkorú törvényes képviselője, a sértett és képviselője másolatot kaphat a szakvéleményről, valamint az olyan nyomozási cselekményről készült iratról, amelyeknél jelenlétüket e törvény lehetővé teszi; az egyéb iratról pedig akkor, ha ez a nyomozás érdekeit nem sérti. A sértett a nyomozás során keletkezett más iratokról a tanúkénti kihallgatását követően kaphat másolatot.

(3) A feljelentő részére - ha nem a (2) bekezdésben felsoroltak valamelyike - csak a szóban tett feljelentésről készített jegyzőkönyvről, illetve az írásban tett feljelentés megtételét igazoló iratról adható másolat. Ha a feljelentő a magyar nyelvet nem ismeri, kérelmére a nyomozó hatóság vagy az ügyész a feljelentés megtételéről igazolást állít ki. Az igazolást a feljelentő részére kézbesíteni kell.

(4) Ha a terheltnek a 179. § (1) bekezdése szerinti kihallgatására, a védő kirendelésére, illetőleg meghatalmazására az irat keletkezését követően került sor, a (2) bekezdés szerinti iratról másolat

kiadására a terhelt az első kihallgatására történő idézés kézbesítésétől, a védő a kirendelésről szóló határozat kézbesítésétől, illetőleg a meghatalmazás benyújtásától fogva jogosult.

(5) A nyomozás befejezését követően

a) a terhelt, a védő és a fiatalkorú törvényes képviselője másolatot kaphat a nyomozás azon iratairól, amelyeknek a megismerésére a 193. § (1) bekezdése alapján jogosult,

b) a sértett és képviselője másolatot kaphat a nyomozás azon iratairól, amelyeknek a megismerésére a 229. § (2) bekezdése alapján jogosult.

(6) A bírósági eljárásban a vádlott, a védő, a fiatalkorú törvényes képviselője, a sértett, a magánvádló, a pótmagánvádló, a magánfél és a felsoroltak képviselője részére - ha e törvény eltérően nem rendelkezik - a másolat kiadása csak a 60. § (1) bekezdésére figyelemmel korlátozható.

(7) Az egyéb érdekelt és képviselője részére az iratokból az őt érintő körben adható másolat. A tanú részére a vallomását tartalmazó jegyzőkönyvről, illetőleg jegyzőkönyv-részről adható másolat. A terhelt, a tanú és az e törvényben meghatározott más személyek érdekében eljáró segítő másolatot kaphat a nyomozás azon iratairól, amelyekről e törvény szerint másolatot kaphat az, akinek érdekében a segítő eljár.

(8) A másolat kiadása ellen nincs helye jogorvoslatnak. A kiadás megtagadása miatt külön jogorvoslatnak van helye.

(9) Az ügy irataiban fel kell jegyezni, hogy másolat kiadására mely iratról, kinek a részére, milyen formában került sor.

(10) Az eljárás jogerős befejezését követően az első fokon eljárt bíróság, a nyomozás megszüntetését követően az ügyész, illetve a nyomozó hatóság, az eljárás megszüntetését vagy a vádemelés részbeni mellőzését követően az ügyész a büntetőeljárásban részt vevő személyek kérelmére - a (6)-(8) bekezdésben meghatározottak szerint - legkésőbb a kérelem előterjesztésétől számított nyolc napon belül az eljárás során keletkezett iratról másolatot ad ki.

(11) Aki az (1)-(7) vagy a (10) bekezdés alapján az eljárás során keletkezett iratról másolatot kaphat, kérheti, hogy a másolatot a bíróság, az ügyész, illetve a nyomozó hatóság elektronikus formában adathordozón vagy az általa megjelölt elektronikus levelezési címre adja ki, ha az

a) elektronikus formában,

b) elektronikus okiratként, vagy

c) a papíralapú okirat elektronikus másolataként

az eljáró bíróságnál, ügyésznél, illetve nyomozó hatóságnál rendelkezésre áll.

(12) A másolat akkor áll elektronikus formában rendelkezésre, ha a bíróság, az ügyész, illetve a nyomozó hatóság a papíralapú iratot információs rendszer alkalmazásával szerkesztette meg. Az elektronikus formában rendelkezésre álló, a (11) bekezdés szerint kiadott másolat nem hiteles.

(13) Ha a másolat (11) bekezdés szerinti elektronikus levelezési címre történő kiadása nem teljesíthető, a bíróság, az ügyész, illetve a nyomozó hatóság a másolatot adathordozón adja ki vagy az indítványozót az általa megjelölt elektronikus levelezési cím útján tájékoztatja arról, hogy az eljárás során keletkezett iratról az (1)-(7) vagy a (10) bekezdés alapján kaphat másolatot.

(14) A másolat kiadására vonatkozó jogosultságok gyakorlása érdekében a bíróság, az ügyész, illetve a nyomozó hatóság a másolat kiadására jogosultak számára az iratokhoz való elektronikus hozzáférés lehetőségét jogszabályban meghatározottak szerint biztosítja.

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

http://njt.hu/cgi_bin/njt_doc.cgi?docid=23938.347581

4. § Az irattári anyaggal rendelkező szervek és a maradandó értékű iratokat őrző természetes személyek kötelesek a szervesen összetartozó irataik egységének, illetve eredeti rendjének megőrzéséről, valamint a tulajdonukban vagy birtokukban lévő maradandó értékű iratok megóvásáról gondoskodni.

5. § (1) Köziratot, valamint közlevéltárban őrzött, köziratnak nem minősülő levéltári anyagot elidegeníteni, megrongálni vagy egyéb módon használhatatlanná tenni, továbbá - a szabályosan lefolytatott selejtezési eljárást, illetve a hiteles másolatkészítési eljárást kivéve - megsemmisíteni tilos.

(2) A megrongálás, az egyéb módon történő használhatatlanná tétel, továbbá a megsemmisítés tilalma a nyilvános magánlevéltárban őrzött levéltári anyagra és a védetté nyilvánított maradandó értékű magániratra is kiterjed.

(3) Az (1) bekezdésben meghatározott elidegenítési tilalom nem zárja ki a közlevéltárban őrzött, köziratnak nem minősülő levéltári anyagnak levéltár, múzeum, könyvtár részére csereszerződés útján történő elidegenítését. A csereszerződés megkötéséhez, valamint a nyilvános magánlevéltárban őrzött magánirat elidegenítéséhez a kultúráért felelős miniszternek engedélye szükséges. A védetté nyilvánított magánirat elidegenítésekor a kulturális örökség védelméről szóló törvényben foglaltak szerint kell eljárni.

(4) Az elektronikus ügyintézés részletszabályairól szóló kormányrendeletnek megfelelően lefolytatott hiteles másolatkészítési eljárást követően, jegyzőkönyv felvétele mellett, a közirat papíralapú példánya megsemmisíthető.

(5) A megsemmisítési jegyzőkönyv tartalmazza:

a) a papíralapú iratról készült hiteles elektronikus példány beazonosítására alkalmas jelölést,
b) a megsemmisítési eljárás alá vont iratok keletkezésének vagy beérkezésének

időintervallumát,

c) a megsemmisítés elrendelésének időpontját,

d) az aláírást és a dátumot.

(6) A (4) bekezdés szerinti megsemmisítési eljárás feltétele a hiteles elektronikus másolatnak az elektronikus ügyintézés részletszabályairól szóló kormányrendeletnek megfelelő elektronikus tárolása, a selejtezhető iratoknak a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló kormányrendelet szerinti szabályos selejtezése, illetve a megsemmisítést kezdeményező szervnek az elektronikus formában tárolt iratok közlevéltári átvételének eljárásrendjéről és műszaki követelményeiről szóló miniszteri rendelet szerinti digitális levéltári átadásra irányuló technikai képessége.

A köziratok kezelésének irányítása

8/A. § A köziratok kezelésének szakmai irányítását a Kormány által kijelölt miniszter látja el.

A köziratok kezelése és védelme

9. § (1) A közfeladatot ellátó szerv köteles

a) a hozzá érkezett és az általa készített iratokat az érkezés, illetve a keletkezés időpontjában nyilvántartásba venni;

b) a nyilvántartást és az ahhoz kapcsolódó - az irattári anyag áttekinthetőségét szolgáló - ügyviteli segédleteket levéltári célra is használható módon vezetni;

c) az ügyintézés során a selejtezhető, valamint a maradandó értékű, s ezért nem selejtezhető iratokat az irattári terv megfelelő tételébe besorolni, a tétel jelét az iraton feltüntetni, és azt a nyilvántartásba bejegyezni;

d) a nála keletkező, nem selejtezhető iratok készítésekor azok tartós megőrzését lehetővé tevő eszközöket, anyagokat és eljárásokat alkalmazni;

e) az elintézett ügyek iratait - az irattári terv szerinti rendszerezés és válogatás pontosságának ellenőrzése mellett - irattárában elhelyezni, s irattári anyagának szakszerű és biztonságos megőrzéséről, valamint használatra bocsátásáról gondoskodni;

f) irattári anyagának selejtezhető részét, az irattári tervben megjelölt irattári őrzési idő letelte után, a szerv nem selejtezhető iratainak átvételére jogosult közlevéltár (a továbbiakban: illetékes közlevéltár) engedélyével kiselejtezni;

g) a nem selejtezhető irattári tételekbe tartozó iratokat a kapcsolódó nyilvántartásokkal és segédletekkel együtt - a 12. §-ban előírtak szerint - saját költségén az illetékes közlevéltárnak átadni.

(2) Elektronikus iratkezelés esetén a közfeladatot ellátó szerv kizárólag olyan iratkezelési szoftvert alkalmazhat, amely a külön jogszabályban meghatározott követelményeknek megfelel és tanúsítvánnyal rendelkezik.

(3) Az (1) bekezdésben meghatározott követelmények teljesítéséért, valamint az iratok szakszerű és biztonságos megőrzésére alkalmas irattár kialakításáért és működtetéséért, továbbá az iratkezeléshez szükséges egyéb tárgyi, technikai és személyi feltételek biztosításáért, valamint a megfelelő tanúsítvánnyal rendelkező iratkezelési szoftver használatáért a közfeladatot ellátó szerv vezetője felelős.

(4) Az e törvényben, valamint a 35/A. § (1) bekezdése szerinti kormányrendeletben meghatározott követelmények teljesítésének részletes szabályait a közfeladatot ellátó szerv által készített egyedi, vagy a részére kötelezően előírt egységes iratkezelési szabályzat és irattári terv (a továbbiakban együtt: iratkezelési szabályzat) tartalmazza.

9/A. § (1) Közfeladatot ellátó szerv megszüntetése vagy feladatkörének megváltoztatása esetén a rendelkező szerv köteles intézkedni az érintett szerv irattári anyagának további elhelyezéséről, biztonságos megőrzéséről, kezeléséről és használhatóságáról.

(2) Ha a megszűnő szerv más szervbe olvad be, iratait a feladatait átvevő szerv irattárában kell elhelyezni.

(3) Ha a megszűnő szerv feladatköre több szerv között oszlik meg, vagy valamely szerv egyes feladatait egy másik szerv veszi át, az irattári anyagot csak irattári tételenként szabad megosztani. Az egyes ügyiratokra vonatkozó igényt másolat készítésével vagy kölcsönzéssel kell teljesíteni. Az irattári anyag irattári tételenkénti megosztását az illetékes közlevéltár egyetértésével kell elvégezni.

(4) Ha a közfeladatot ellátó szerv jogutód nélkül szűnik meg, irattári anyagának maradandó értékű részét az illetékes közlevéltárban kell elhelyezni. Az irattári anyag többi részének meghatározott ideig történő további őrzéséhez, kezeléséhez és selejtezéséhez szükséges költségek biztosításáról a megszüntetésről intézkedő szerv gondoskodik.

335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről

http://njt.hu/cgi_bin/njt_doc.cgi?docid=96458.345675

A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (a továbbiakban: Ltv.) 35/A. §-a (1) bekezdésében foglalt felhatalmazás alapján a közfeladatot ellátó szervek iratkezelésének általános követelményeiről a Kormány a következőket rendeli el:

A rendelet hatálya

1. § (1) E rendelet hatálya a közfeladatot ellátó szervekre és - a (2) bekezdésben foglalt korlátozással - azok irattári anyagára terjed ki. E rendelet határozza meg a közfeladatot ellátó szervekhez beérkező és az ott keletkezett papír alapú és elektronikus köziratok (a továbbiakban: irat) kezelésének egységes követelményeit, továbbá a központi államigazgatási szervek, az önkormányzati hivatalok és az önkormányzati társulások iratkezelési szabályzatai végrehajtásának ellenőrzési rendjét.

(2) E rendelet rendelkezéseit a minősített iratokra és azok kezelési rendjére külön jogszabályban foglalt eltérésekkel kell alkalmazni.

(3) E rendelet rendelkezéseit az elektronikus ügyintézés esetén az elektronikus ügyintézés részletszabályairól szóló kormányrendeletben foglalt eltérésekkel kell alkalmazni.

(4) E rendelet rendelkezéseit a bírósági iratkezelésre a bírósági ügyviteli és iratkezelési szabályokról szóló szabályokban foglalt eltérésekkel kell alkalmazni.

2. § E rendelet alkalmazásában

1. *ÁNYK űrlap benyújtás támogatás szolgáltatás:* a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet szerinti szolgáltatás;

4. *biztonságos kézbesítési szolgáltatás:* a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet szerinti szabályozott biztonságos kézbesítési szolgáltatás;

5a. *egységes kormányzati ügyiratkezelő rendszer:* az iratkezelés e rendeletben meghatározott egyes fázisainak elvégzésére irányuló szolgáltatások, informatikai, technológiai és személyi feltételek összessége, amelyben a Kormány által arra kijelölt működtető szerv és szolgáltató biztosítja:

a) a postai úton érkező, papíralapú küldemények átvételét, felbontását, érkeztető azonosítóval történő ellátását, a küldemények hiteles elektronikus irattá történő átalakítását, érkeztető nyilvántartásba való bevezetését, a címzett részére elektronikus úton történő megküldését,

b) elektronikus irat hiteles papíralapú irattá történő alakítására irányuló szolgáltatást;

10. *elektronikus tájékoztatás:* az információs önrendelkezési jogról és az információszabadságról szóló törvény szerint előírt elektronikus közzétételi kötelezettség;

11. *elektronikus ügyintézés:* a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvény szerinti elektronikus ügyintézés;

12. *elektronikus ügyintézési felügyelet:* a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet szerinti hatóság;

13. *elektronikus űrlapok:* a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet szerinti elektronikus adatbeviteli felület;

14. *elektronikus visszaigazolás:* olyan - kiadmánynak nem minősülő - elektronikus dokumentum, amely az elektronikus úton érkezett irat átvételéről és az érkeztetés azonosítójáról, valamint a külön jogszabályban meghatározott egyéb adatokról is értesíti annak küldőjét;

28. *kézbesítési szolgáltatás:* a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet szerinti kézbesítési szolgáltatás;

44. *szabályozott elektronikus ügyintézési szolgáltatás:* a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvény szerinti szolgáltatás;

6. § A közfeladatot ellátó szervek iratkezelését úgy kell megszervezni, hogy:

a) a szervhez érkezett, ott keletkező, illetve onnan továbbított irat azonosítható, fellelési helye, útja követhető, ellenőrizhető és visszakereshető legyen;
b) az irat tartalma csak az arra jogosult számára legyen megismerhető;
c) az irat kezeléséért fennálló személyi felelősség egyértelműen megállapítható legyen;
d) az irat szakszerű kezeléséhez, nyilvántartásához, kézbesítéséhez, védelméhez szükséges személyi, tárgyi, technikai feltételek biztosítottak legyenek;
e) a beérkezett és továbbított iratok megváltoztathatatlansága biztosított legyen;
f) a rendszeres selejtezés elvégzésével az irattári iratanyag felesleges felhalmozódása megelőzhető, a maradandó értékű iratok megőrzése biztosított legyen;
g) az ügyintézéshez, a döntések előkészítéséhez, a szervezet rendeltetésszerű működéséhez megfelelő támogatást biztosítson.

16. § (1) A közfeladatot ellátó szerv adottságainak és igényeinek megfelelően az iratkezelést

(2) A szerv az elintézett ügyek iratait irattárában helyezi el.

16/A. § (1) A közfeladatot ellátó szerv az iratkezelési feladatokat saját maga láthatja el, vagy annak támogatására a szabályozott elektronikus ügyintézési szolgáltatást biztosító szolgáltató (a továbbiakban: SZEÜSZ szolgáltató) által biztosított elektronikus iratok kezelése szolgáltatást vehet igénybe, amely esetben a SZEÜSZ szolgáltató a közfeladatot ellátó szerv adatfeldolgozójaként jár el.

(2) Ha a közfeladatot ellátó szerv az elektronikus iratok kezelését az elektronikus dokumentumtárolási szolgáltatás igénybevételével biztosítja, úgy az iratkezelési szoftverfunkciók közös informatikai rendszerben elkülönítés nélkül is kialakíthatóak, az irattározás - ha az ahhoz szükséges információk már rendelkezésre állnak - automatizálható.

(3) Ha a közfeladatot ellátó szerv egyes iratkezelési feladatokat szakrendszeri ügyintézést támogató informatikai rendszer alkalmazásával lát el, az ezzel összefüggő eljárást az iratkezelési szabályzatban köteles előírni.

16/B. § (1) Ha a közfeladatot ellátó szerv csak papír alapú iratokat kezel, és iratkezelési szoftvert használ, köteles biztosítani az iratkezelési szoftverben tárolt valamennyi információnak az elektronikus ügyintézés részletes szabályairól szóló jogszabály szerinti elektronikus dokumentumformátumban történő automatikus előállítását.

19. § A küldemény átvételére jogosult:

a) a címzett vagy az általa megbízott személy;
b) a szerv vezetője vagy az általa megbízott személy;
c) az iratkezelést felügyelő vezető vagy az általa megbízott személy;
d) a postai meghatalmazással rendelkező személy;
e) az ügyfélszolgálati iroda munkatársa;
f) hivatali munkaidőn túl az ügyeleti szolgálatot teljesítő személy;
g) a SZEÜSZ-ként biztosított elektronikus iratok kezelése szolgáltatással a szolgáltatást végző, a központi érkeztetési ügynök szolgáltatással vagy az alkalmazott iratkezelési szoftverrel a központi érkeztetési ügynököt vagy az iratkezelési szoftvert használó;
h) a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (a továbbiakban: Ket.) 169/A. § (3) bekezdés *a)* pontjában meghatározott szervezet.

20. § (1) A küldeményt átvevő köteles ellenőrizni:

21. § (1) Az átvevő a papír alapú iratok esetében a kézbesítőokmányon aláírásával és az átvétel dátumának, valamint nevének olvasható feltüntetésével az átvételt elismeri. Az „azonnal” és „sürgős” jelzésű küldemények átvételi idejét óra, perc pontossággal kell megjelölni, amit a kézbesítőokmányon kívül az átvett küldeményen is rögzíteni kell.

(2) Elektronikus úton, nem biztonságos kézbesítési szolgáltatás igénybevételével érkezett küldemények esetében az átvevő a feladónak - ha azt kéri és elektronikus válaszcímét megadja - haladéktalanul elküldi a küldemény átvételét igazoló és az érkeztetés egyedi azonosítóját is tartalmazó elektronikus visszaigazolást.

(3) A biztonságos kézbesítési szolgáltatás, illetve az ÁNYK űrlap benyújtás támogatás szolgáltatás igénybevételével érkezett küldemények és az elektronikus űrlapok esetében az átvétel visszaigazolása az elektronikus ügyintézés részletes szabályairól szóló kormányrendeletben, valamint a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendeletben (a továbbiakban: SZEÜSZR) meghatározottak szerint történik.

(4) A Ket. szerinti ügyintézési rendelkezés által érintett eljárásokban az elektronikus úton érkezett irat átvételét (érkeztetését) és hitelességének ellenőrzését követően a közfeladatot ellátó szerv - ha a küldő az azonosításához szükséges adatait megadta - az ügyintézési rendelkezések

nyilvántartásában ellenőrzi, hogy a küldő az elektronikus kapcsolattartást, illetve annak alkalmazott módját választotta. Ha a küldő nem az elektronikus kapcsolattartást, illetve annak alkalmazott módját választotta, a közfeladatot ellátó szerv az iratot nem tekinti benyújtottnak, és erről a küldőt az (5) bekezdés szerint értesíti.

(5) A küldőt a közfeladatot ellátó szerv az irat befogadásának elutasításáról:

a) ha a küldő az azonosításához szükséges adatait megadta, az ügyintézési rendelkezésében megadott elektronikus elérhetőségén, az ott előírt módon,

b) ennek hiányában, ha a küldő közölte a válaszadási elektronikus postafiók címét, úgy elektronikus levélben,

c) egyéb esetben papír alapon értesíti.

(2) (6) Ha a küldő az elektronikus ügyintézési rendelkezésében igényli az időszaki értesítést, úgy a nevében történt, a (4) bekezdés és a 25. § szerint elutasított benyújtás tényét az értesítésben szerepeltetni kell.

(7) Amennyiben iratkezelésre nem jogosult személy vagy szervezeti egység veszi át a küldeményt, úgy azt - a Ket. 169/A. § (3) bekezdése alapján meghatározott szervezet kivételével - köteles haladéktalanul, de legkésőbb az érkezést követő első munkanap kezdetén az illetékes iratkezelési egységnek az iratkezelési szabályzat szerinti kezelése céljából átadni.

25. § (1) Az elektronikus úton, a nem biztonságos kézbesítési szolgáltatás, illetve az ÁNYK űrlap benyújtás támogatás szolgáltatás igénybevételével megküldött küldemény átvételét meg kell tagadni, ha az biztonsági kockázatot jelent a fogadó szerv informatikai rendszerére.

(2) A küldemény a fogadó szerv rendszerére biztonsági kockázatot jelent, ha

a) a hatóság informatikai rendszeréhez vagy azon keresztül más informatikai rendszerhez való jogosulatlan hozzáférés célját szolgálja, vagy

b) az *a)* pontban meghatározott informatikai rendszer üzemelésének vagy más személyek hozzáférésének jogosulatlan akadályozására irányul,

c) az *a)* pontban meghatározott informatikai rendszerben lévő adatok jogosulatlan megváltoztatására, hozzáférhetetlenné tételére vagy törlésére irányul.

(3) A fogadó szerv a feldolgozás elmaradásának tényéről és annak okáról a 21. § (5) bekezdésében meghatározott formában értesíti a küldőt.

(4) Nem köteles a fogadó szerv a (3) bekezdés szerint értesíteni a feladót, ha korábban már érkezett azonos jellegű biztonsági kockázatot tartalmazó küldemény az adott küldőtől. Az ismétlődés értelmezésére vonatkozó szabályokat a belső szabályzat tartalmazza.

(5) Az átvett, de az átvételt követő ellenőrzés alapján biztonsági kockázatot jelentő elektronikus küldemények esetében a fogadó szerv a további feldolgozást megszakítja, és a küldőt a biztonsági kockázat miatti feldolgozás elutasításról a 21. § (5) bekezdésében meghatározott formában értesíti.

26. § (1) Téves címzés, sikertelen vagy helytelen kézbesítés esetén a küldeményt azonnal továbbítani kell a címzetthez, vagy ha ez nem lehetséges:

a) papír alapú küldemény esetén vissza kell küldeni a feladónak,
b) elektronikus küldemény esetén a 25. § (3) bekezdésében foglaltak szerint kell eljárni.

(2) Ha a feladó nem állapítható meg, a küldeményt a 25. § (1) bekezdésben jelzett kivétellel, irattárazni és az irattári tervben meghatározott idő után selejtezni kell.

A küldemény felbontása és érkeztetése

27. § (1) A közfeladatot ellátó szervhez érkezett küldeményt

a) a címzett, vagy
b) a központi iratkezelést felügyelő vezető által írásban felhatalmazott személy, vagy
c) a szervezeti és működési szabályzatban vagy iratkezelési szabályzatban meghatározottak szerint a szervezeti egység foglalkoztatottja, vagy az arra feljogosított személy, vagy
d) automatikusan a SZEÜSZ szolgáltató által biztosított elektronikus iratok kezelése szolgáltatás vagy az alkalmazott iratkezelési szoftver

bonthatja fel.

(2) A közfeladatot ellátó szerv - az egységes kormányzati ügyiratkezelő rendszer érkeztető rendszerében történő érkeztetés kivételével - az érkeztetést és felbontást saját maga láthatja el, vagy ahhoz a SZEÜSZR-ben meghatározott SZEÜSZ szolgáltató szolgáltatását veheti igénybe.

(3) Ha a közfeladatot ellátó szerv a papír alapú küldemények fogadására olyan szolgáltatót vesz igénybe, amely:

a) a SZEÜSZR alapján a papír alapú irat hiteles elektronikus irattá alakítását úgy nyújtja, hogy elvégzi az elektronikus másolatnak a közfeladatot ellátó szerv részére történő továbbítását, és
b) a közfeladatot ellátó szerv a külön jogszabály alapján az eredeti papír alapú irat ügyfél részére történő visszaadásáról rendelkezett,

a közfeladatot ellátó szerv a továbbiakban iratként a hiteles elektronikus másolatot kezeli.

33. § (4) Ha a papír alapú küldemények fogadására a közfeladatot ellátó szerv olyan szolgáltatót vesz igénybe, amely külön jogszabály alapján a papír alapú irat hiteles elektronikus irattá alakítását úgy biztosítja, hogy egyúttal vállalja az elektronikus másolat továbbítását, úgy az irat elektronikus másolatához a (2) és (3) bekezdés szerinti esetekben a boríték hiteles elektronikus másolatát is csatolni kell.

Egységes kormányzati ügyiratkezelő rendszer

38/A. § (1) Az egységes kormányzati ügyiratkezelő rendszer

a) érkeztető rendszere (a továbbiakban: érkeztető rendszer) biztosítja az 1. mellékletben felsorolt szervek címére érkezett postai papíralapú küldemények tekintetében a 2. § 5a. pont *a)* alpontja szerinti feladatok ellátását,

b) a kijelölt szolgáltató útján biztosítja az 1. mellékletben felsorolt szervek expediálásra előkészített, papíralapú kézbesítést igénylő elektronikus iratainak hiteles papíralapú irattá történő alakítását a 2. mellékletben felsorolt küldemények kivételével.

(2) Az (1) bekezdés *b)* pontja szerinti szolgáltató az elektronikus irat átvételéről, az elektronikus irat hiteles papír alapú irattá történő alakítást követően az irat kézbesítés céljára történő átadásáról szóló elektronikus visszajelzésében az elektronikus iratot feladó szervet az elektronikus irathoz rendelt azonosító kód feltüntetésével értesíti.

38/B. § (1) Az érkeztető rendszerben a postai szolgáltatótól a papíralapú küldeményt az 1. mellékletben felsorolt szervek címére érkezett postai papíralapú küldeményeken szereplő címhez rendelt, az érkeztető rendszer működtetője szervezeti és működési szabályzatában meghatározott kézbesítési ponton az érkeztető rendszer működtetője szervezeti és működési szabályzatában arra feljogosított személy veszi át.

(2) Ha az érkeztető rendszerhez olyan küldemény érkezik, amelynek nem az 1. mellékletben felsorolt szerv a címzettje, az érkeztető rendszer működtetője a küldeményeket dokumentáltan, felbontás nélkül, kézbesítés céljából a postai szolgáltatónak haladéktalanul visszaadja.

(3) Az érkeztető rendszer működtetője a (2) bekezdés szerint jár el abban az esetben is, amennyiben a küldemény címzettje nem állapítható meg.

(4) Ha az érkeztető rendszerhez a 2. mellékletben felsorolt küldemény érkezik, azt az érkeztető rendszer működtetője az átvétel tényének és időpontjának megjelölésével, illetve amennyiben a küldeményt felbontotta, a felbontás tényének és időpontjának dokumentálásával a címzetthez a postai papíralapú küldeményeken feltüntetett címen történő közvetlen kézbesítés érdekében - a közvetlen kézbesítés szükségességének küldeményen való feltüntetése mellett - a postai szolgáltatónak haladéktalanul visszaadja vagy az Állami Futárszolgálatnak haladéktalanul átadja.

(5) A (4) bekezdés szerinti küldeményeket az 1. melléklet szerinti szerv köteles átvenni, illetve ha a küldemények között tévesen továbbított küldemény található, azt haladéktalanul továbbítja a helyes címzett részére.

38/C. § (1) Az érkeztető rendszer működtetője a küldeményt felbontás után - a 2. mellékletben felsorolt küldemény kivételével - érkeztetési azonosítóval látja el, gondoskodik a hiteles elektronikus irattá (ezen alcím alkalmazásában a továbbiakban: elektronikus irat) alakításáról és az elektronikus iratot bevezeti az elektronikus érkeztetési nyilvántartásba.

(2) Az érkeztető rendszer működtetője a 34. § (2) bekezdés *a)-c)* és *e)* pontjában felsorolt adatokat tartalmazó érkeztetési nyilvántartást elektronikusan, címzett szerint vezeti.

(3) Az egy küldeményben érkező, de különböző címzetteknek szóló iratokat külön kell érkeztetési azonosítóval ellátni és az érkeztetési nyilvántartásba bevezetni.

38/D. § (1) Az érkeztető rendszer működtetője az elektronikus iratot, annak képi ellenőrzését követően az érkeztetési nyilvántartás adataival együtt megküldi a címzett iratkezelési szoftverének.

(1a) Az érkeztető rendszer által tévesen továbbított küldeményt a fogadó szerv a címzettnek elektronikus úton haladéktalanul átadja és az átadásról az érkeztető rendszert haladéktalanul értesíti. Ha a tévesen továbbított küldeményről a címzett nem állapítható meg vagy a címzett nem az 1. mellékletben felsorolt szerv, a fogadó szerv az érkeztető rendszer működtetőjét erről a tényről haladéktalanul értesíti és a küldeményt az iratkezelő rendszerből törli.

(2) Az érkeztető rendszer működtetője az érkeztető rendszerben érkeztetett papíralapú iratot száznyolcvan napig tárolja. Az érkeztető rendszer működtetője a tárolás ideje alatt a tárolt iratot a címzett vagy a feladó kérésére dokumentáltan, a kérelemben megjelölt módon, a kérelmező költségére átadja.

(3) A tárolt iratot a tárolási idő leteltét követő kilencven napon belül az érkeztető rendszer működtetője az 1. mellékletben felsorolt szervvel egyeztetett módon irattározás céljából átadja.

(4) A küldemények visszakereshetőségét, sérülésmentes és jogosulatlan hozzáférést megakadályozó tárolását a feladónak vagy a címzettnek történő átadásig biztosítani kell.

38/E. § (1) Az érkeztető rendszer technológiai vagy informatikai rendszerében fellépő átmeneti üzemzavar elhárítását követően az üzemzavar ideje alatt átvett küldemények tekintetében az érkeztető rendszer működtetője az elektronikus irat címzetthez történő megküldéséhez szükséges, még el nem végzett feladatokat haladéktalanul elvégzi.

(2) A tartós, huszonnégy órát meghaladó üzemzavarról, valamint az üzemzavar megszűnéséről - a küldeményeknek közvetlenül a címzetthez való továbbítása, illetve az üzemzavar elhárítását követően az új küldemények érkeztető rendszerben történő ismételt fogadása érdekében - az érkeztető rendszer működtetője a Magyar Posta Zrt.-t haladéktalanul értesíti.

(3) Az érkeztető rendszer működtetője az önálló iratkezelési rendjében meghatározott módon az átmeneti és tartós üzemzavarról az 1. mellékletben felsorolt szerveket is értesíti.

(4) A tartós üzemzavar ideje alatt átvett papíralapú küldeményeket az érkeztető rendszer működtetője a postai szolgáltató útján haladéktalanul megküldi a címzettnek.

(5) A címzett az iratkezelési szoftverét érintő, az elektronikus irat fogadását akadályozó üzemzavarról haladéktalanul értesíti az érkeztető rendszer működtetőjét. Az üzemzavar elhárításáról szóló értesítést követően az érkeztető rendszer működtetője a már megküldött küldeményeket ismételten továbbítja.

38/F. § (1) Az érkeztető rendszeren keresztül megküldött elektronikus irat az ügyintézési határidő számítása szempontjából a címzetthez történő megérkezéskor minősül beérkezettnek.

(2) Az érkeztető rendszer üzemeltetője a tértivevényes küldeményeket soron kívül dolgozza fel, a visszaérkezett tértivevényekről készült elektronikus iratot soron kívül küldi meg a könyvelt postai küldemény feladójának.

(3) Az érkeztetési nyilvántartás az érkeztetési adatokat az adott évi érkeztetési állomány lezárását követően egy évig tárolhatja. Ezt követően az adatokat törölni kell.

38/G. § (1) E rendeletnek az expediálásra vonatkozó rendelkezéseit a (2) bekezdésben foglalt eltérésekkel kell alkalmazni.

(2) Az 1. mellékletben felsorolt szerv az 55. §-ban meghatározott iratkezelési feladatainak ellátását követően, a papíralapú kézbesítést igénylő elektronikus küldeményeket a szabályozott elektronikus ügyintézési szolgáltatást végző kijelölt szolgáltatónak adja át az elektronikus irat hiteles papíralapú irattá alakítása és címzetthez történő kézbesítése érdekében.

38/H. § (1) Az 1. melléklet szerinti szervek a 38/A. § (1) bekezdés *b)* pontjában meghatározott szolgáltatóhoz megküldésre kerülő elektronikus iraton Magyarország hivatalos címerén kívül más, a szerv egyedi megkülönböztetésére használt jelzést nem tüntethetnek fel, e szervek a szolgáltatónak a papír alapú irat borítékjának ilyen jellegű jelzéssel történő ellátására irányuló kézbesítési utasítást nem adhatnak.

(2) Az 1. melléklet szerint szerveknél a 38/A. § (1) bekezdés *b)* pontjában meghatározott szolgáltató részére megküldött elektronikus iratot a lapok sorszámozása mellett úgy kell megszerkeszteni, hogy laponként a lap felső részéből legalább 5 milliméter, jobb és bal oldalából legalább 10 milliméter, alsó részéből legalább 20 milliméter a papír alapú irat kötelező elemeinek elhelyezése céljából elhagyásra kerüljön. Bármilyen nyomtatható információ, ide értve a fej- és láblécet, a lábjegyzetet és az oldalszámot is csak ebben a keretben helyezhető el.

(3) Az 1. melléklet szerinti szerveknek a 38/A. § (1) bekezdés *b)* pontjában meghatározott szolgáltató részére megküldött elektronikus irattal kapcsolatos kézbesítési utasításban jelezniük kell:

a) az elektronikus irat lapjainak számát,
b) a küldemény típusát (pl. sima, ajánlott küldemény),
c) a postai feladáshoz szükséges egyéb utasításokat (pl. elsőbbségi küldemény),
d) amennyiben az irat színes formátumú megjelenítést igényel, úgy az erre vonatkozó információkat.

53. § (6) Ha jogszabály a kiadmányozó aláírását, illetve bélyegzőlenyomatát követeli meg, úgy az elektronikus iratról készült hiteles papír alapú iraton ez úgy teljesíthető, hogy az irat utolsó lapján, vagy külön lapon - a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló Korm. rendeletben előírt záradékon felül - az 1. mellékletben felsorolt szervek által elhelyezett záradékként szerepelnie kell

a) a kiadmányozó külön jogszabályban meghatározott követelményeknek megfelelő elektronikus aláírásának és az aláírás időpontja képi lenyomatának,

b) a kiadmányozó neve melletti „s.k.” jelzésnek, valamint a szervezet nevében történő gépi aláírásnak és az aláírás időpontja képi lenyomatának, vagy

c) az iratérvényességi nyilvántartásban történő nyilvántartás ténye feltüntetésének és a kiadmányozó neve mellett az „s.k.” jelzésnek.

56. § (1) A küldeményeket a továbbítás módja szerint kell csoportosítani (posta, kézbesítő, futárszolgálat útján, személyesen vagy elektronikus formában).

(2) Ha a szerv az irat kézbesítésére a SZEÜSZR-ben meghatározott kézbesítési SZEÜSZ szolgáltatót vesz igénybe, a kézbesítés a szolgáltató részére történő átadással történik.

57. § Az elektronikus iratok kézbesítésének rendjét a közfeladatot ellátó szerv az iratkezelési szabályzatában - az adott közfeladatot ellátó szervre és eljárására vonatkozó, továbbá az elektronikus iratok kézbesítését előíró jogszabályi rendelkezések figyelembevételével - határozza meg.

Selejtezés

64. § (1) Az ügyiratok selejtezését az iratkezelés felügyeletével megbízott vezető által kijelölt legalább 3 tagú selejtezési bizottság javaslata alapján lehet elvégezni az irattári tervben rögzített őrzési idő leteltével.

(6) Elektronikus dokumentumkezelés esetén az adatbázisban levő iratok metaadatainak selejtezése fizikai törlés nélkül, a selejtezés tényére vonatkozó megjelöléssel történik. A selejtezést követően az elektronikus dokumentumokat meg kell semmisíteni, azaz visszaállíthatatlanul törölni kell az adatállományból.

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.338522

1. § (1) E törvény alkalmazásában

1. *adat:* az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

2. *adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

3. *adatfeldolgozó:* az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

3a. *adatgazda:* annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;

4. *adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők rögzítése;

5. *adatkezelő:* az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

6. *adminisztratív védelem:* a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

7. *auditálás:* előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

8. *bizalmasság:* az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

9. *biztonsági esemény:* 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;

10. *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;

11. *biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége;

12. *biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

13. *biztonsági szint:* a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

14. *biztonsági szintbe sorolás:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

14b. *elektronikus információs rendszer:* az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;

15. *elektronikus információs rendszer biztonsága:* az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

16. *életciklus:* az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

17. *észlelés:* a biztonsági esemény bekövetkezésének felismerése;

18. *felhasználó:* egy adott elektronikus információs rendszert igénybe vevők köre;

19. *fenyegetés:* olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

20. *fizikai védelem:* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

21. *folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

25. *információ:* bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

26. *kiberbiztonság:* a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez;

27. *kibervédelem:* a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

28. *kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

29. *kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

30. *kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

31. *kockázatokkal arányos védelem:* az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

38. *rendelkezésre állás:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

39. *sértetlenség:* az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

40. *sérülékenység:* az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

41. *sérülékenységvizsgálat:* az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;

41a. *súlyos biztonsági esemény:* olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

43. *szervezet:* az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető;

44. *teljes körű védelem:* az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

45. *üzemeltető:* az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

48. *zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem.

2. § (1) E törvény rendelkezéseit kell alkalmazni:

a) a központi államigazgatási szervekre, a Kormány és a kormánybizottságok kivételével,
b) a Köztársasági Elnöki Hivatalra,
c) az Országgyűlés Hivatalára,
d) az Alkotmánybíróság Hivatalára,
e) az Országos Bírósági Hivatalra és a bíróságokra,
f) az ügyészségekre,
g) az Alapvető Jogok Biztosának Hivatalára,
h) az Állami Számvevőszékre,
i) a Magyar Nemzeti Bankra,
j) a fővárosi és megyei kormányhivatalokra,
k) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalaira, a hatósági igazgatási társulásokra,
l) a Magyar Honvédségre.

(2) E törvény rendelkezéseit kell alkalmazni:

a) az (1) bekezdésben meghatározott szervek és ezen szervek számára adatkezelést végzők,

elektronikus információs rendszereinek védelmére.

4. § Az elektronikus információs rendszerekre és eszközökre, szervezetekre nemzetközi egyezmények vagy nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján kiadott biztonsági tanúsítványokat a hatóság az eljárása során figyelembe veszi.

3. Alapvető elektronikus információbiztonsági követelmények

5. § Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

6. § Az elektronikus információs rendszernek az 5. §-ban meghatározott feltételeknek megfelelő védelme körében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

a) a megelőzést és a korai figyelmeztetést,
b) az észlelést,
c) a reagálást,
d) a biztonsági események kezelését.

4. Az elektronikus információs rendszerek biztonsági osztályba sorolása

7. § (1) Annak érdekében, hogy az e törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából.

(2) A biztonsági osztályba sorolás alkalmával - az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján - 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.

(3) A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni.

(4) Az elektronikus információs rendszer bizalmasság, sértetlenség és rendelkezésre állás szerinti biztonsági osztálya alapján kell megvalósítani az 5. és 6. §-ban előírt védelmi intézkedéseket az adott elektronikus információs rendszerre vonatkozóan.

(5) A szervezet vezetője az e törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.

(6) Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek elektronikus információs rendszerei tekintetében az e törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb biztonsági osztály is megállapítható.

8. § (1) A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

(2) A soron kívüli biztonsági osztályba sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén szükséges elvégezni. A soron kívüli felülvizsgálatot akkor is el kell végezni, ha a szervezet státuszában, illetve az általa kezelt vagy feldolgozott adatok vonatkozásában változás következik be.

(3) A 7. § (2) bekezdésében foglaltakkal összhangban előírt, az elektronikus információs rendszerre vonatkozó védelem elvárt erősségének eléréséhez a szervezetnek lehetősége van a biztonsági intézkedések fokozatos kivitelezésére. Ennek keretében az első vizsgálatkor

megállapított biztonsági osztályt alapul véve, minden egyes következő, magasabb biztonsági osztályhoz rendelt biztonsági intézkedések kivitelezésére két év áll rendelkezésére.

(5) Ha a szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, akkor a vizsgálatot követő 90 napon belül cselekvési tervet készít a hiányosság megszüntetésére.

(6) A hatóság a szervezet által megállapított biztonsági osztályt - a 2. § (3)-(6) bekezdésében meghatározott elektronikus információs rendszerek kivételével - felülbírálhatja és magasabb, indokolt esetben alacsonyabb szintű osztályba sorolást is megállapíthat.

(7) Új elektronikus információs rendszer bevezetése vagy már működő elektronikus információs rendszer fejlesztése során megállapított biztonsági osztályhoz tartozó követelményeket a használatbavételig teljesíteni kell.

5. Az elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintje

9. § (1) A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján a szervezetnek biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint.

(2) Az elektronikus információs rendszer

a) fejlesztését végző,
b) üzemeltetését végző,
c) üzemeltetéséért felelős vagy
d) információbiztonságáért felelős

szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő biztonsági szintekbe kell sorolni jogszabályban meghatározott szempontok szerint.

(3) A szervezet vagy szervezeti egységek biztonsági szintjét a szervezet védelemre való felkészültsége határozza meg.

(4) A szervezet vagy szervezeti egységek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint.

(5) A szervezet vagy szervezeti egység az e törvényben meghatározott feltételeknek megfelelő, az adott szervezetre irányadó besorolási szintnél magasabb szintű besorolást is megállapíthat.

(6) Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek szervezetei tekintetében az e törvényben meghatározott feltételeknek megfelelő, az adott szervezetre irányadó besorolási szintnél magasabb, a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb szintű besorolás is megállapítható.

10. § (1) A szervezet vagy szervezeti egység jogszabályban meghatározott szempontok alapján meghatározza, hogy a vizsgálat elvégzésekor melyik biztonsági szintnek felel meg.

(2) Ha a vizsgálat alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre vagy szervezeti egységre jogszabályban meghatározott biztonsági szint, akkor a szervezetnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére.

(3) A szervezet vagy a 9. § (2) bekezdése szerinti szervezeti egység biztonsági szintjét a cselekvési tervben szereplő ütemezés szerint kell elérni. Ha a biztonsági szint a vizsgálat alapján az 1. szintet nem éri el, az 1. szint eléréséhez szükséges intézkedéseket az (1) bekezdésben meghatározott szempontok szerint lefolytatott vizsgálatot követő öt éven belül meg kell valósítani.

(4) A 9. § (2) bekezdésében előírt biztonsági szint teljesítése során a szervezetnek lehetősége van az előírt biztonsági szint fokozatos elérésére. Ennek keretében a magasabb biztonsági szint elérésére - minden egyes szintet érintően, a következő magasabb szintre lépéshez - két év áll rendelkezésére.

(5) A biztonsági szint meghatározását a 9. § (1) bekezdésében előírt biztonsági szint elérését követően legalább háromévenként, szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

(6) Az elektronikus információs rendszer biztonságát érintő változás esetén, illetve új elektronikus információs rendszer bevezetésekor a szervezet vagy szervezeti egység biztonsági szintbe sorolását soron kívül meg kell ismételni.

(7) Ha a soron kívüli felülvizsgálat alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre vagy szervezeti egységre előírt biztonsági szint, akkor a szervezetnek vagy szervezeti egységnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére.

(8) A szervezet vagy felelős szervezeti egység biztonsági szintbe sorolását a szervezet vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági szintbe sorolás eredményét a szervezet informatikai biztonsági szabályzatában vagy szervezeti egységre irányadó szabályzatban kell rögzíteni.

6. A szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségei

11. § (1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a

jogszabályban meghatározott követelmények teljesülését,

b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,

c) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,

f) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,

g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,

h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,

i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

j) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,

k) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

l) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

m) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,

n) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

(2) Az (1) bekezdésben meghatározott feladatokért a szervezet vezetője az (1) bekezdés *k)* és *l)* pontjában meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni.

(3) A jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybevétele esetén az (1) és (2) bekezdésben meghatározott feltételek teljesítését a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve a központi adatkezelő és adatfeldolgozó szolgáltató úgy biztosítja, hogy közreműködik a szervezet és az elektronikus információs rendszer biztonságáért felelős személy feladatai ellátásában a jogkörébe tartozó tevékenységek tekintetében. A két szervezet közötti feladatmegosztást kétoldalú szolgáltatási szerződések biztosítják, amelyek a központi szolgáltató felett felügyeletet gyakorló miniszter

vagy megbízottja ellenjegyzésével lépnek hatályba. Az (1) bekezdés *a)* és *b)* pontjában meghatározott feladatok keretében a szervezeti szintű informatikai biztonsági szabályok kidolgozása abban az esetben is a szervezet vezetőjének felelőssége, ha a jogszabály által kijelölt központosított elektronikus és hírközlési szolgáltatót vesz igénybe.

(5) A nemzetbiztonsági védelem alá eső állami szervek esetében az elektronikus információs rendszer biztonságáért felelős személy kinevezése tekintetében a kormányzati eseménykezelő központ előzetes véleményezési jogot gyakorol.

(6) A biztonsági esemény kivizsgálásában részt vevő személy csak az lehet, aki rendelkezik a szervezet vezetője által - a kormányzati eseménykezelő központ előzetes véleményezésével - kiadott megbízással. A megbízást írásba kell foglalni. A biztonsági esemény kivizsgálásában részt vevő személynek a megbízás előtt részt kell vennie a biztonságiesemény-kezelő eljárásról szóló, kormányzati eseménykezelő központ által tartott tájékoztató előadáson.

(7) A polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei, valamint a honvédelmi célú elektronikus információs rendszerek esetében az (5) és (6) bekezdés rendelkezései nem alkalmazhatóak.

12. § A szervezet vezetője köteles együttműködni a hatósággal. Ennek során:

a) a 11. § (1) bekezdés *c)* pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,
b) a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,
c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja

a hatóság részére.

13. § (1) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

(2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
b) elvégzi vagy irányítja az *a)* pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

(3) Az elektronikus információs rendszer biztonságáért felelős személy e törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

(4) Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

(5) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését

a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők

e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

(6) Az elektronikus információs rendszer biztonságáért felelős személy e törvény szerinti feladatai és felelőssége az (5) bekezdés szerinti esetekben más személyre nem átruházható.

(7) Az elektronikus információs rendszer biztonságáért felelős személy jogosult az (5) bekezdés szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

(8) A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.

(9) A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.

(10) Nem kell a (8) bekezdés szerinti képzettséget megszereznie annak a személynek, aki rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.

(11) Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.

III. FEJEZET
AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI FELÜGYELETE

7. Az elektronikus információs rendszerek biztonságának felügyelete

14. § (1) Az e törvény hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét - a 2. § (3)-(6) bekezdésében meghatározott kivétellel - a Kormány által kijelölt hatóság látja el.

(2) A hatóság feladata:

a) az osztályba sorolás és a biztonsági szint megállapításának ellenőrzése és az ellenőrzés eredménye alapján döntés meghozatala,

b) az elektronikus információs rendszerek osztályba sorolására és a szervezetek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzése,

c) az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése, és eredményességének ellenőrzése,

d) a rendelkezésre álló információk alapján kockázatelemzés elvégzése,

e) a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálására irányuló hatósági eljárás megindítása,

f) javaslattétel a létfontosságú rendszerek és létesítmények védelmi szabályozását biztosító, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény szerinti ágazati kijelölő hatóság részére a nemzeti létfontosságú rendszerelem kijelölésére,

h) együttműködés az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvényben meghatározott elektronikus ügyintézési felügyelettel a szabályozott elektronikus ügyintézési szolgáltatás szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében,

i) kapcsolattartás az elektronikus információbiztonság területén a nemzetbiztonsági szolgálatokkal,

j) kapcsolattartás a 19. § (1)-(4) bekezdésében meghatározott eseménykezelő központokkal,

(3) A hatóság eljárásainak általános ügyintézési határideje - a (3a) bekezdésben meghatározott kivétellel - 30 nap.

(3a) A hatóság által lefolytatott hatósági eljárás ügyintézési határideje a logikai védelmi kötelezettség teljesítésére irányuló vizsgálat esetén százhúsz nap.

(3b) A hatóság eljárásaiban

a) az ügyfél értesítése az eljárás megindításáról mellőzhető,

b) a szervezet köteles a szakértői eljárásban közreműködni.

(4) A (2) bekezdés *a)* és *b)* pontjában foglalt feladatok ellátása körében a hatóság javaslatára az e-közigazgatásért felelős miniszter az informatikáért felelős miniszter egyetértésével, valamint a minősített adatok védelmének szakmai felügyeletéért felelős miniszter és a katasztrófák elleni védekezésért felelős miniszter javaslatainak figyelembevételével éves ellenőrzési tervet (a továbbiakban: éves ellenőrzési terv) készít.

7. Az elektronikus információs rendszerek biztonságának felügyelete

15. § (1) A hatóság nyilvántartja és kezeli

a) a szervezet azonosításához szükséges adatokat,

b) a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatait,

c) a szervezetnek az elektronikus információs rendszer biztonságáért felelős személye természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail címét, a 13. § (8) bekezdésében meghatározott végzettségét,

d) a szervezet informatikai biztonsági szabályzatát,

e) a biztonsági eseményekkel kapcsolatos, a kormányzati eseménykezelő központtól kapott

értesítéseket.

(2) Az (1) bekezdésben meghatározott adatok kezelésének célja az elektronikus információs rendszerek védelmével kapcsolatos kötelezettségek teljesítése és hatósági ellenőrzésének biztosítása.

(3) A szervezet az (1) bekezdés *a)-c)* pontjában meghatározott adatokat és ezek változásait, valamint az (1) bekezdés *d)* pontja szerinti szabályzatot megküldi a hatóságnak a nyilvántartásba vétel érdekében.

(4) Az (1) bekezdésben meghatározott nyilvántartásból - ha jogszabály eltérően nem rendelkezik - adattovábbítás kizárólag a 19. § (1)-(4) bekezdésében meghatározott eseménykezelő központok részére végezhető.

(5) Ha a szervezet e törvény hatálya alá tartozó tevékenységet már nem végez, akkor az (1) bekezdésben meghatározott adatokat a hatóság a tevékenység befejezése bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

(6) Ha az (1) bekezdésben meghatározott adatok változását a szervezet bejelenti, akkor az eredeti adatokat a hatóság az adat változása bejelentését követő öt év elteltével köteles a nyilvántartásból törölni.

16. § (1) A hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult megtenni, elrendelni, ellenőrizni minden olyan, az elektronikus információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek. Ennek érdekében jogosult:

a) az érintett szervezeteknél a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,
b) a követelményeknek való megfelelőség alátámasztásához szükséges dokumentumokat bekérni, illetve a 12. § *b)* pontja alapján megküldött dokumentációt felülvizsgálni,
c) a 7-8. § szerinti biztonsági osztályba sorolást, a 9-10. § szerinti biztonsági szint megállapítását, vagy a védelmi intézkedéseket ellenőrizni, az ott feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni,
d) a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában ellenőrizni az információbiztonsági követelmények megtartását,
e) hazai információbiztonsági, kibervédelmi gyakorlatokat szervezni,
f) a nemzetközi információbiztonsági, kibervédelmi gyakorlatokon felkérésre képviselni Magyarországot,
g) véleményezési jogot gyakorolni a kormányzati eseménykezelő központnak az ágazatok közötti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban.

(2) A (3) bekezdésben meghatározott kivétellel, ha a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a hatóság

a) köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére,
b) ha az *a)* pontban meghatározottak ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, az eset összes körülményeinek mérlegelésével bírságot szabhat ki, amely további nem teljesülés esetén megismételhető.

(4) Ha az elektronikus információs rendszert olyan

a) súlyos biztonsági esemény éri vagy
b) súlyos biztonsági esemény közvetlen bekövetkezése fenyegeti,

amely a rendszert működtető szervezet működéséhez szükséges alapvető információk vagy személyes adatok sérülésével jár, a kormányzati eseménykezelő központ a védelmi feladatainak

ellátása érdekében kötelezheti a szervezetet, hogy a súlyos biztonsági esemény megszüntetése vagy a fenyegetettség elhárítása érdekében szükséges intézkedéseket tegye meg.

(5) Ha a szervezethez információbiztonsági felügyelő van kirendelve, a (4) bekezdés szerinti körülmények felmerüléséről a kormányzati eseménykezelő központot haladéktalanul tájékoztatja. Azonnali beavatkozást igénylő esetben a kormányzati eseménykezelő központ - az információbiztonsági felügyelő útján - az információk sérülésének elkerüléséhez szükséges mértékben ideiglenes intézkedést alkalmazhat.

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.338504

Az Országgyűlés az információs önrendelkezési jog és az információszabadság biztosítása érdekében, a személyes adatok védelmét, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jog érvényesülését szolgáló alapvető szabályokról, valamint az ezen szabályok ellenőrzésére hivatott hatóságról az Alaptörvény végrehajtására, az Alaptörvény VI. cikke alapján a következő törvényt alkotja:

2. A törvény hatálya

2. § (1) E törvény hatálya a Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik.

(2) E törvényt a teljesen vagy részben automatizált eszközzel, valamint a manuális módon végzett adatkezelésre és adatfeldolgozásra egyaránt alkalmazni kell.

(3) E törvényben foglaltakat kell alkalmazni, ha az Európai Unió területén kívül személyes adatok kezelését folytató adatkezelő az adatfeldolgozással Magyarország területén székhellyel, telephellyel, fióktelepével vagy lakóhellyel, tartózkodási hellyel rendelkező adatfeldolgozót bíz meg, vagy itt lévő eszközt használ fel, kivéve, ha ez az eszköz csak az Európai Unió területén átmenő adatforgalom célját szolgálja. Az ilyen adatkezelőnek Magyarország területén képviselőt kell kineveznie.

3. § E törvény alkalmazása során:

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

2. személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális

azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

3. különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

4. bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

5. közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

6. közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

7. hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

8. tiltakozás: az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

9. *adatkezelő:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

10. *adatkezelés:* az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat

további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

11. *adattovábbítás:* az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

12. *nyilvánosságra hozatal:* az adat bárki számára történő hozzáférhetővé tétele;

13. *adattörlés:* az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

14. *adatmegjelölés:* az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

15. *adatzárolás:* az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

16. *adatmegsemmisítés:* az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;

17. *adatfeldolgozás:* az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik;

18. *adatfeldolgozó:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

19. *adatfelelős:* az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

20. *adatközlő:* az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi;

21. *adatállomány:* az egy nyilvántartásban kezelt adatok összessége;

22. *harmadik személy:* olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval;

4. § (1) Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.

(2) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

(3) A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

5.Az adatkezelés jogalapja

5. § (1) Személyes adat akkor kezelhető, ha

a) ahhoz az érintett hozzájárul, vagy
b) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés).

(2) Különleges adat a 6. §-ban meghatározott esetekben, valamint akkor kezelhető, ha

a) az adatkezeléshez az érintett írásban hozzájárul,
b) a 3. § 3. pont a) alpontjában foglalt adatok esetében az törvényben kihirdetett nemzetközi szerződés végrehajtásához szükséges, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli, vagy
c) a 3. § 3. pont b) alpontjában foglalt adatok esetében törvény közérdeken alapuló célból elrendeli.

(3) Kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

(4) Kizárólag állami vagy önkormányzati szerv kezelheti az állam bűncselekmények megelőzésére és üldözésére irányuló, valamint közigazgatási és igazságszolgáltatási feladatainak ellátása céljából kezelt bűnügyi személyes adatokat, valamint a szabálysértési, a polgári peres és nemperes ügyekre vonatkozó adatokat tartalmazó nyilvántartásokat.

6. § (1) Személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése

a) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy
b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

(4) Ha a hozzájáruláson alapuló adatkezelés célja az adatkezelővel írásban kötött szerződés végrehajtása, a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából - e törvény alapján - az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételének tényét. A szerződésnek

félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul adatainak a szerződésben meghatározottak szerinti kezeléséhez.

(5) Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a felvett adatokat törvény eltérő rendelkezésének hiányában

a) a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy
b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll

további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

(6) Az érintett kérelmére, kezdeményezésére indult bírósági vagy hatósági eljárásban az eljárás lefolytatásához szükséges személyes adatok tekintetében, az érintett kérelmére indult más ügyben az általa megadott személyes adatok tekintetében az érintett hozzájárulását vélelmezni kell.

(7) Az érintett hozzájárulását megadottnak kell tekinteni az érintett közszereplése során általa közölt vagy nyilvánosságra hozatalra általa átadott személyes adatok tekintetében.

(8) Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

6.Az adatbiztonság követelménye

7. § (1) Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.

(2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

(3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

(4) A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok - kivéve ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

(5) A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja

a) a jogosulatlan adatbevitel megakadályozását;

b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

(6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

8. Az adatkezelés korlátai

9. § (1) Ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusának rendelkezése alapján az adatkezelő személyes adatot akként vesz át, hogy az adattovábbító adatkezelő az adattovábbítással egyidejűleg jelzi a személyes adat

a) kezelésének lehetséges célját,
b) kezelésének lehetséges időtartamát,
c) továbbításának lehetséges címzettjeit,
d) érintettje e törvényben biztosított jogainak korlátozását, vagy
e) kezelésének egyéb korlátozását

(a továbbiakban: együtt: adatkezelési korlátozás), a személyes adatokat átvevő adatkezelő (a továbbiakban: adatátvevő) a személyes adatot az adatkezelési korlátozásnak megfelelő terjedelemben és módon kezeli, az érintett jogait az adatkezelési korlátozásnak megfelelően biztosítja.

(2) Az adatátvevő az adatkezelési korlátozásra tekintet nélkül is kezelheti a személyes adatot és biztosíthatja az érintett jogait, ha ahhoz az adattovábbító adatkezelő előzetes hozzájárulását adta.

9. Adatfeldolgozás

10. § (1) Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit e törvény, valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel.

(2) Az adatfeldolgozó az adatkezelő rendelkezése szerint vehet igénybe további adatfeldolgozót.

(3) Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

(4) Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

10.Automatizált adatfeldolgozással hozott döntés

11.§ (1) Kizárólag automatizált adatfeldolgozással az érintett személyes jellemzőinek értékelésén alapuló döntés meghozatalára csak akkor kerülhet sor, ha a döntést

a) valamely szerződés megkötése vagy teljesítése során hozták, feltéve hogy azt az érintett kezdeményezte, vagy
b) olyan törvény teszi lehetővé, amely az érintett jogos érdekeit biztosító intézkedéseket is megállapítja.

(2) Az automatizált adatfeldolgozással hozott döntés esetén az érintettet - kérelmére - tájékoztatni kell az alkalmazott módszerről és annak lényegéről, valamint az érintettnek álláspontja kifejtésére lehetőséget kell biztosítani.

13. Az érintettek jogai és érvényesítésük

14. § Az érintett kérelmezheti az adatkezelőnél

a) tájékoztatását személyes adatai kezeléséről,
b) személyes adatainak helyesbítését, valamint
c) személyes adatainak - a kötelező adatkezelés kivételével - törlését vagy zárolását.

15. § (1) Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

(1a) Az adatkezelő - ha belső adatvédelmi felelőssel rendelkezik, a belső adatvédelmi felelős útján - az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

(1b) Az elektronikus hírközlésről szóló törvény hatálya alá tartozó adatkezelő az (1a) bekezdésben meghatározott kötelezettségét az elektronikus hírközlésről szóló törvényben meghatározott, a személyes adatok megsértésének eseteit tartalmazó nyilvántartás vezetésével is teljesítheti.

(2) Az adatkezelő az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

(3) Az (1a) és a (2) bekezdés szerinti adatok nyilvántartásban való megőrzésére irányuló - és ennek alapján a tájékoztatási - kötelezettség időtartamát az adatkezelést előíró jogszabály korlátozhatja. E korlátozás körében személyes adatok esetében öt évnél, különleges adatok esetében pedig húsz évnél rövidebb időtartam nem állapítható meg.

(4) Az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 25 napon belül, közérthető formában, az érintett erre irányuló kérelmére írásban megadni a tájékoztatást.

(5) A (4) bekezdésben foglalt tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet az adatkezelőhöz még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg. A költségtérítés mértékét a felek között létrejött szerződés is rögzítheti. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy a tájékoztatás kérése helyesbítéshez vezetett.

14. Az érintett előzetes tájékoztatásának követelménye

20. § (1) Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező.

(2) Az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

(3) Kötelező adatkezelés esetén a tájékoztatás megtörténhet a (2) bekezdés szerinti információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

(4) Ha az érintettek személyes tájékoztatása lehetetlen vagy aránytalan költséggel járna, a tájékoztatás megtörténhet az alábbi információk nyilvánosságra hozatalával is:

a) az adatgyűjtés ténye,

b) az érintettek köre,
c) az adatgyűjtés célja,
d) az adatkezelés időtartama,
e) az adatok megismerésére jogosult lehetséges adatkezelők személye,
f) az érintettek adatkezeléssel kapcsolatos jogainak és jogorvoslati lehetőségeinek ismertetése, valamint
g) ha az adatkezelés adatvédelmi nyilvántartásba vételének van helye, az adatkezelés nyilvántartási száma, kivéve a 68. § (2) bekezdésében foglalt esetet.

18. Belső adatvédelmi felelős és adatvédelmi szabályzat

24. § (1) Az adatkezelő, illetve az adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó - jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező - belső adatvédelmi felelőst kell kinevezni vagy megbízni

a) az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetve feldolgozó adatkezelőnél és adatfeldolgozónál;
b) a pénzügyi szervezetnél;
c) az elektronikus hírközlési és közüzemi szolgáltatónál.

(2) A belső adatvédelmi felelős

a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
b) ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;
c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;
e) vezeti a belső adatvédelmi nyilvántartást;
f) gondoskodik az adatvédelmi ismeretek oktatásáról.

(3) Az (1) bekezdésben meghatározott adatkezelőknek, valamint - az adatvédelmi nyilvántartásba bejelentési kötelezettség alá nem eső adatkezelők kivételével - egyéb állami és önkormányzati adatkezelőknek e törvény végrehajtása érdekében adatvédelmi és adatbiztonsági szabályzatot kell készíteniük.

35. Adatvédelmi nyilvántartás

65. § (1) Az adatkezelő személyes adatokra vonatkozó adatkezeléseiről, az érintettek tájékozódásának elősegítése érdekében a Hatóság hatósági nyilvántartást (a továbbiakban:

adatvédelmi nyilvántartás) vezet, amely - a (2) bekezdésben meghatározott kivételekkel - tartalmazza

a) az adatkezelés célját,
b) az adatkezelés jogalapját,
c) az érintettek körét,
d) az érintettekre vonatkozó adatok leírását,
e) az adatok forrását,
f) az adatok kezelésének időtartamát,
g) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló adattovábbításokat is,
h) az adatkezelő, valamint az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
i) az alkalmazott adatfeldolgozási technológia jellegét,
j) a belső adatvédelmi felelős alkalmazása esetén annak nevét és elérhetőségi adatait.

(2) Az adatvédelmi nyilvántartás a nemzetbiztonsági szervek adatkezelései tekintetében a nemzetbiztonsági szerv nevét és címét, az adatkezelés célját és jogalapját tartalmazza.

(3) Nem vezet adatvédelmi nyilvántartást a Hatóság arról az adatkezelésről, amely

a) az adatkezelővel munkaviszonyban, tagsági viszonyban, óvodai nevelésben való részvételre irányuló, tanulói vagy tanulószerződéses jogviszonyban, kollégiumi tagsági viszonyban vagy - a pénzügyi szervezetek, közüzemi szolgáltatók, elektronikus hírközlési szolgáltatók ügyfelei kivételével - ügyfélkapcsolatban álló személyek adataira vonatkozik;
b) a bevett egyház belső szabálya szerint történik;
c) az egészségügyi ellátásban kezelt személy betegségével, egészségi állapotával kapcsolatos személyes adatokra vonatkozik gyógykezelés vagy az egészség megőrzése, társadalombiztosítási igény érvényesítése céljából;
d) az érintett anyagi és egyéb szociális támogatása céljából nyilvántartott személyes adatokra vonatkozik;
e) a hatósági, az ügyészségi és a bírósági eljárás által érintett személyeknek az eljárás lefolytatásával kapcsolatos személyes adataira, vagy a büntetés-végrehajtás során a büntetés- végrehajtással összefüggésben kezelt személyes adatokra vonatkozik;
f) a hivatalos statisztika célját szolgáló személyes adatokat tartalmaz, feltéve hogy - törvényben meghatározottak szerint - az adatok érintettel való kapcsolatának megállapítását véglegesen lehetetlenné teszik;
g) a médiaszolgáltatásokról és a tömegkommunikációról szóló törvény szerinti médiatartalom-szolgáltató olyan adatait tartalmazza, amelyek kizárólag saját tájékoztatási tevékenységét szolgálják;
h) a tudományos kutatás céljait szolgálja, ha az adatokat nem hozzák nyilvánosságra,
i) a levéltári őrizetbe vett iratokkal összefüggésben valósul meg.

(4) Az adatvédelmi nyilvántartás nyilvános, abba bárki betekinthet, az abban foglaltakról feljegyzést készíthet.

66. § (1) A személyes adatok kezelésének nyilvántartásba vételét az adatkezelő - a kötelező adatkezelés kivételével az adatkezelés megkezdése előtt - kérelmezi a Hatóságnál. A kötelező adatkezelés, valamint a 68. § (2) bekezdésben foglalt eset kivételével az adatkezelés a nyilvántartásba vételt megelőzően nem kezdhető meg.

(2) A kötelező adatkezelés nyilvántartásba vételét az adatkezelő az adatkezelést elrendelő jogszabály hatálybalépését követő húsz napon belül kérelmezi a Hatóságnál.

(3) A nyilvántartásba vétel szempontjából az eltérő célú adatkezelések önálló adatkezelésnek minősülnek, abban az esetben is, ha a kezelt adatok köre azonos.

(4) A nyilvántartásba vétel iránti kérelemnek tartalmaznia kell a 65. § (1), illetve (2) bekezdése szerinti adatokat.

68. § (1) A (3) bekezdésben foglalt kivétellel a Hatóság az adatkezelést a kérelem megérkezésétől számított nyolc napon belül nyilvántartásba veszi, ha a kérelem tartalmazza a 65. § (1), illetve (2) bekezdése szerinti adatokat.

(2) A (3) bekezdésben foglalt kivétellel ha a Hatóság a nyilvántartásba vétel iránti kérelmet határidőben nem bírálja el, az adatkezelő az adatkezelést a kérelemben foglaltak szerint megkezdheti.

(3) A (4) és (5) bekezdés szerinti adatkezelést a Hatóság a kérelem megérkezésétől számított negyven napon belül nyilvántartásba veszi, ha a kérelem tartalmazza a 65. § (1), illetve (2) bekezdése szerinti adatokat és az adatkezelőnél a jogszerű adatkezelés feltételei biztosíthatók.

(4) Ha a kérelem olyan - az (5) bekezdésben meghatározott - adatkezelés nyilvántartásba vételére irányul, amely az adatkezelő korábban nyilvántartásba vett adatkezelésével nem érintett adatállományra vonatkozik, illetve amely az adatkezelő korábban nyilvántartásba vett adatkezelésénél nem alkalmazott, új adatfeldolgozási technológia alkalmazását teszi szükségessé, a nyilvántartásba vétel feltétele, hogy az adatkezelőnél a jogszerű adatkezelés feltételei biztosíthatók legyenek.

(5) A (4) bekezdésben foglalt nyilvántartásba vételi feltétel, az abban meghatározottak szerint

a) az országos hatósági, munkaügyi és bűnügyi adatállományok kezelésére;
b) a pénzügyi szervezetek és közüzemi szolgáltatók ügyfelekre vonatkozó adatkezelésére;
c) az elektronikus hírközlési szolgáltatóknak a szolgáltatást igénybe vevőkre vonatkozó adatkezelésére

vonatkozik.

(6) A Hatóság az adatvédelmi nyilvántartásba vételi kérelemnek helyt adó határozatának tartalmaznia kell az adatkezelés nyilvántartási számát, amelyet az adatkezelőnek az adatok

minden továbbításánál, nyilvánosságra hozásánál és az érintettnek való kiadásakor fel kell tüntetni. A nyilvántartási szám az adatkezelés azonosítására szolgál, és nem tanúsítja a nyilvántartásba vett adatkezelés jogszerűségét.

(7) A 65. § (1) bekezdés *b)-j)* pontja szerinti adatok megváltozása esetén az adatkezelő a változás bekövetkezésétől számított nyolc napon belül változásbejegyzési kérelmet nyújt be a Hatóságnak. A változásbejegyzési eljárásra az (1), (3) és (5) bekezdésben foglalt szabályokat megfelelően alkalmazni kell, azzal, hogy a kérelemnek csak a megváltozott adatokat kell tartalmaznia.

36. Adatvédelmi audit

69. § (1) Az adatvédelmi audit a Hatóság olyan szolgáltatása, amelynek célja a végzett vagy tervezett adatkezelési műveletek a Hatóság által meghatározott és közzétett szakmai szempontok szerinti értékelésén keresztül a magas szintű adatvédelem és adatbiztonság megvalósítása. Tervezett adatkezelési műveletek akkor vonhatók audit alá, ha az adatkezelésre vonatkozó koncepció kidolgozottsága ezt lehetővé teszi.

(2) Adatvédelmi auditot a Hatóság az adatkezelő kérelmére folytathat le. Az adatvédelmi audit lefolytatása iránti kérelem benyújtását követő tizenöt napon belül az adatvédelmi audit lefolytatásáért fizetendő ellenérték mértékét és az adatvédelmi audit elvégzésének várható időpontját a Hatóság közli az adatkezelővel. A Hatóság az adatvédelmi auditot abban az esetben folytatja le, ha a Hatóság közlését követő tizenöt napon belül az adatkezelő nyilatkozik arról, hogy a Hatóság közlésében megállapított feltételek ismeretében az adatvédelmi audit lefolytatása iránti kérelmét fenntartja.

(3) Az adatvédelmi audit lefolytatásáért fizetendő ellenérték mértékét - az elvégzendő tevékenység mértékével arányosan - a Hatóság állapítja meg, az azonban nem haladhatja meg az ötmillió forintot. Az adatvédelmi audit lefolytatásáért fizetendő ellenérték a Hatóság bevétele.

(4) Az adatvédelmi audit eredményét a Hatóság az auditról készített értékelésben rögzíti. Az értékelés javaslatokat fogalmazhat meg az adatkezelő számára. Az értékelés tartalma az üzleti titokra alkalmazandó szabályok szerint ismerhető meg, az adatkezelő erre irányuló kérelmére azonban a Hatóság honlapján - a kérelemnek megfelelően - az értékelést vagy az értékelés összegző megállapításait közzéteszi.

(5) Az adatvédelmi audit a Hatóság e törvényben rögzített egyéb hatásköreinek gyakorlását nem korlátozza.

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

http://njt.hu/cgi_bin/njt_doc.cgi?docid=176705.349727

8. § (1) Az európai uniós támogatásból, központi költségvetési támogatásból megvalósuló fejlesztési projektek információbiztonsági követelményeinek teljesítése során a projekt vezetője, a projekt tervezési szakaszában a hatóság részére véleményezésre megküldi a fejlesztendő elektronikus információs rendszerre vonatkozó biztonsági osztályba sorolást, továbbá mindazon dokumentációkat, amelyek alapján a biztonsági követelmények megvalósulása ellenőrizhető a projekt teljes életciklusára nézve, ideértve az átvétel vagy teljesülés után az elektronikus információs rendszer használata során érvényesítendő elvárásokat is.

(2) A projekt szintű mérföldkövek figyelembevételével, az adott projektszakasz zárását megelőző legkevesebb harminc nappal kell a hatóság rendelkezésére bocsátani a kapcsolódó elektronikus információbiztonsági dokumentációt annak érdekében, hogy a hatóság észrevételei vagy kifogásai a projekt terveken, vagy a projekt tárgyán átvezethető és alkalmazható legyen.

(3) A hatvan napnál rövidebb időtartamú projektek esetén az (1) bekezdés szerinti dokumentációt legkésőbb a projekt befejezésekor kell a hatóság rendelkezésére bocsátani. A projekt megvalósítása során - elektronikus információs rendszer érintettsége esetén - a hatósággal a projekt tartalmáról egyeztetni kell.

(4) A hatóság az (1) bekezdés szerinti dokumentumok tekintetében más hatóság véleményét kikérheti.

5. Az érintett szervezet egyes kötelezettségei

11. § (1) Az érintett szervezet, ha az elektronikus információs rendszer biztonságért felelős személy, szervezet kijelölése vagy az elektronikus informatikai biztonsági szabályzat elkészítése a jogszabályban meghatározott időn belül neki fel nem róható okból nem teljesül, a jogszabályban meghatározott határidőn belül a hatóságot tájékoztatja a teljesítést akadályozó ok és a teljesítés határidejének megjelölésével.

(2) Az elektronikus információs rendszer biztonságáért felelős személy - ideértve az információbiztonsági szolgáltatást nyújtó vállalkozás tagjait és alkalmazottait is - az érintett szervezet igényeihez igazodva és annak rendelkezése szerint feladatát elláthatja

a) részmunkaidőben,
b) a vonatkozó szerződésben meghatározott időtartamban, vagy
c) több érintett szervezetnél.

(3) Az elektronikus információs rendszer biztonságáért felelős személyről szóló, az Ibtv. 12. § *a)* pontja szerinti tájékoztatás magában foglalja a vonatkozó munka-, megbízási vagy más szerződés másolatának hatóság kérésére való megküldését olyan módon, hogy abból csak a hatóság számára releváns, a feladat- és hatásköre ellátáshoz szükséges információ legyen megismerhető. A szerződéshez csatolni kell az adott személy végzettségét, képzettségét igazoló okirat, vagy a szakterületi gyakorlatot igazoló okirat vagy nyilatkozat másolatát.

(4) A jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybevétele során - figyelemmel az Ibtv. 11. § (3) bekezdésére - az érintett szervezet vezetője nem mentesül a jogszabályban meghatározott azon kötelezettségek alól, amelyek az érintett szervezet felett az információbiztonság tekintetében gyakorolt irányítási és ellenőrzési jogkörébe tartoznak.

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

http://njt.hu/cgi_bin/njt_doc.cgi?docid=176725.332228

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (2) bekezdés *a)* pontjában kapott felhatalmazás alapján, a Kormány tagjainak feladat- és hatásköréről szóló 152/2014. (VI. 6.) Korm. rendelet 21. § 5. és 20. pontjában meghatározott feladatkörömben eljárva - a Kormány tagjainak feladat- és hatásköréről szóló 152/2014. (VI. 6.) Korm. rendelet 109. § 11. pontjában meghatározott feladatkörében eljáró nemzeti fejlesztési miniszterrel egyetértésben - a következőket rendelem el:

1. § Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó elektronikus információs rendszerrel rendelkező szervezet az elektronikus információs rendszereit az 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.

2. § Az elektronikus információs rendszerrel rendelkező szervezet vagy e szervezetnek az Ibtv. 9. § (2) bekezdése szerinti szervezeti egysége (a továbbiakban: szervezeti egység) a biztonsági szintbe sorolást a 2. melléklet szerinti biztonsági szintek alapján végzi el.

3. § (1) Az 1. § és a 2. § szerint elvégzett besorolás alapján az elektronikus információs rendszerrel rendelkező szervezet a 3. mellékletben meghatározott, az elektronikus információs rendszerére érvényes biztonsági osztályhoz rendelt követelményeket a 4. mellékletben meghatározott módon teljesíti.

(2) Ha az elektronikus információs rendszerrel rendelkező szervezetre vagy a szervezeti egységre e rendelet előírásai szerint kidolgozott szabályzatokban meghatározott adminisztratív és fizikai védelmi intézkedésektől egy elektronikus információs rendszer esetében a magasabb védelmi igény miatt el kell térni, az eltéréseket az érintett elektronikus információs rendszer e rendelet előírásai szerint kidolgozott szabályzatában kell rögzíteni.

(3) Ha a szervezeti egységre vonatkozóan - a magasabb védelmi igény miatt a szervezetre megállapított biztonsági szinttől - eltérő biztonsági szint megállapítása indokolt, a szervezeti egységet önállóan kell szintbe sorolni a 2. mellékletben meghatározott szempontok alapján.

(4) Ha az elektronikus információs rendszerrel rendelkező szervezet az elektronikus információs rendszernek csak egyes elemeit vagy funkcióit üzemelteti vagy használja - részben vagy teljesen -, a 4. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.

(5) Ha az elektronikus információs rendszert több szervezet használja, az elektronikus információs rendszer üzemeltetője az üzemeltetés elektronikus információbiztonságához szükséges követelményeket az elektronikus információs rendszeren tevékenységet végző minden, elektronikus információs rendszerrel rendelkező szervezet tekintetében érvényesíti.

(6) Az elektronikus információs rendszer üzemeltetője az üzemeltetés elektronikus információbiztonságához szükséges követelményeket úgy érvényesíti az elektronikus információs rendszeren tevékenységet végző elektronikus információs rendszerrel rendelkező szervezetek tekintetében, hogy a követelményeknek való megfelelés az elektronikus információs rendszerrel rendelkező szervezet elektronikus információbiztonsággal kapcsolatos eljárási rendjébe beépüljön. Az elektronikus információs rendszer üzemeltetője és az elektronikus információs rendszerrel rendelkező szervezetek az üzemeltetés elektronikus információbiztonságához szükséges követelményeket az elektronikus információs rendszer üzemeltetésére kötött szerződésben rögzítik.

6. § (1) Ha az elektronikus információs rendszerrel rendelkező szervezet az Ibtv. 26. §-ában meghatározott határidőig az elektronikus információs rendszereinek biztonsági osztályba sorolását elvégezte és az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről szóló BM rendelet 5. § (1) bekezdés *b)* és *c)* pontja szerinti bejelentési kötelezettségének eleget tett, az elektronikus információs rendszerek e rendelet szerinti osztályba sorolását az Ibtv. 8. § (1) bekezdésében foglalt esetekben kell elvégezni.

(2) Ha az elektronikus információs rendszerrel rendelkező szervezet az Ibtv. 26. §-ában meghatározott határidőig a szervezet biztonsági szintbe sorolását elvégezte és a biztonsági szint - az e rendelet 2. mellékletében foglaltak alkalmazásával - nem változik, továbbá az Ibtv. 9. § (2) bekezdése szerinti szervezeti egység nem kerül kijelölésre, valamint az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről szóló BM rendelet 5. § (1) bekezdés *a)* pontja szerinti

bejelentési kötelezettségének eleget tett, a szervezet e rendelet szerinti osztályba sorolását az Ibtv. 10. § (5) bekezdésében foglalt esetekben kell elvégezni.

(3) Ha az elektronikus információs rendszer fejlesztése e rendelet hatálybalépésekor az R. előírásai szerint már folyik, az elektronikus információs rendszer e fejlesztésére az e rendeletben foglaltakat 2015. október 1. napjától kell alkalmazni.

1. melléklet a 41/2015. (VII. 15.) BM rendelethez

Az elektronikus információs rendszerek biztonsági osztályba sorolása

1. Általános irányelvek

1.1. Az érintett szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal érvényesíti;

1.1.1. a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki;

1.1.2. a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen;

1.1.3. a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.

1.2. Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A Nemzeti Elektronikus Információbiztonsági Hatóság ajánlásként kockázatelemzési módszertanokat adhat ki. Ha a szervezet saját kockázatelemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni.

2. Biztonsági osztályok

2.1. A jogszabályban meghatározott biztonsági osztályba sorolás elvégzése a következő elvek figyelembevételével az érintett szervezet felelőssége. A 2.2.-2.6. pontok a döntéshez csak iránymutatást képeznek:

2.2. Az 1. biztonsági osztály esetében csak jelentéktelen káresemény következhet be, mivel

2.2.1. az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;

2.2.2. nincs bizalomvesztés, a probléma az érintett szervezeten belül marad, és azon belül meg is oldható;

2.2.3. a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez képest jelentéktelen;

2.3. A 2. biztonsági osztály esetében csekély káresemény következhet be, mivel

2.3.1. személyes adat sérülhet;

2.3.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;

2.3.3. a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;

2.3.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 1%-át.

2.4. A 3. biztonsági osztály esetében közepes káresemény következhet be, mivel

2.4.1. különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek;

2.4.2. az érintett szervezet üzlet-, vagy ügymenete szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;

2.4.3. a lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;

2.4.4. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 5%-át.

2.5. A 4. biztonsági osztály esetében nagy káresemény következhet be, mivel

2.5.1. különleges személyes adat nagy mennyiségben sérülhet;

2.5.2. személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);

2.5.3. az érintett szervezet üzlet-, vagy ügymenete szempontjából nagy értékű, üzleti titkot, vagy különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet;

2.5.4. a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, vagy vezetésében személyi felelősségre vonást kell alkalmazni;

2.5.5. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 10%-át.

2.6. Az 5. biztonsági osztály esetében kiemelkedően nagy káresemény következhet be, mivel

2.6.1. különleges személyes adat kiemelten nagy mennyiségben sérülhet;

2.6.2. emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;

2.6.3. a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;

2.6.4. az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;

2.6.5. a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

2.6.6. az érintett szervezet üzlet- vagy ügymenete szempontjából nagy értékű üzleti titkot, vagy kiemelten érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;

2.6.7. a közvetlen és közvetett anyagi kár eléri az érintett szervezet költségvetésének 15%-át.

2. melléklet a 41/2015. (VII. 15.) BM rendelethez

Az elektronikus információs rendszerrel rendelkező szervezetek vagy szervezeti egységek biztonsági szintbe sorolása

1. Az érintett szervezet biztonsági szintje 1., ha a szervezet nem üzemeltet és nem fejleszt elektronikus **1. Az 1.érintett szervezet biztonsági szintje 1.,** ha a szervezet nem üzemeltet és nem fejleszt információs rendszert, és saját hatáskörben erre más szervezetet vagy szolgáltatót (ide nem értve a telekommunikációs szolgáltatót) sem vesz igénybe. Az adatfeldolgozás módját nem maga határozza meg, az adatkezelés tekintetében technikai vagy információtechnológiai döntést nem hoz, a használt elektronikus információs infrastruktúra kialakítása tekintetében döntési jogköre - ide nem értve a szervezet munkavégzését érintő informatikai rendszerelemek elhelyezését - nincs, egyedi adatokat és információkat kezel vagy dolgoz fel, és kritikus adatot nem kezel. A szervezet információbiztonsági tevékenysége elsődlegesen az elektronikus információs rendszerrel kapcsolatba kerülő személyek információbiztonsággal kapcsolatos kötelezettségeinek szabályozására, számonkérésére terjed ki, addig a

mértékig, ameddig a szervezet vagy az egyes személyek tevékenysége az elektronikus információs rendszerre hatást tud gyakorolni.

1.1. Az 1. biztonsági szervezeti szint követelményei:

1.1.1. az érintett szervezet az érintett személyi kör részére biztosítja az 1.1.3. pont szerinti szervezeti vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasítását, belső rendelkezését, szabályozását vagy más erre célra szolgáló dokumentumot (a továbbiakban együtt: szabályzat);

1.1.2. az informatikai biztonsági szabályzat része a folyamatos kockázatelemzési eljárás, amely tartalmazza a beépített ellenőrzési pontokat;

1.1.3. az informatikai biztonsági szabályzat vonatkozhat egész szervezetre és működési területére, vagy meghatározott vagyonelemre vagy szervezeti egységre;

1.1.4. a informatikai biztonsági szabályzatot a szervezetre érvényes rendelkezések szerint az erre jogosult vezetőnek kell jóváhagynia;

1.1.5. a informatikai biztonsági szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;

1.1.6. az informatikai biztonsági szabályzat be nem tartása jogkövetkezményt von maga után.

2. Az érintett szervezet biztonsági szintje 2., ha a szervezet vagy szervezeti egység az 1. szinthez rendelt jellemzőkön túl olyan elektronikus információs rendszert használ, amely személyes adatokat kezel, és a szervezet jogszabály alapján kijelölt szolgáltatót vesz igénybe.

2.1. A 2. biztonsági szervezeti szint követelményei az 1. szinthez rendelt követelményeken túl:

2.1.1. az érintett szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak;

2.1.2. a 2.1.1. pont szerinti eljárásrend tartalmazza a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;

2.1.3. az egyes folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és szervezeti egységek tekintetében;

2.1.4. az egyes folyamatokat szervezeti egységek vagy személyek felügyelete alá kell rendelni, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel vagy szervezeti egységekkel;

2.1.5. a folyamatokat és végrehajtásukat úgy kell dokumentálni, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi körét - megállapítható legyen.

3. Az érintett szervezet biztonsági szintje 3., ha a szervezet vagy szervezeti egység a 2. szinthez rendelt jellemzőkön túl szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt. A szervezet kritikus adatot, nem minősített, de 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.

3.1. A 3. biztonsági szervezeti szint követelményei a 2. szinthez rendelt követelményeken túl:

3.1.1. az érintett szervezet a biztonsági kontroll folyamataiba bevonja, és feladataikról, a velük szemben támasztott elvárásokról tájékoztatja a folyamatokban résztvevő személyeket;

3.1.2. a 3.1.1. pont szerinti folyamatokat az érintett szervezet vagy szervezeti egység tekintetében szabályozottan és ellenőrizhető módon kell bevezetni, az érintett személyek számára oktatás tárgyává tenni;

3.1.3. a 3.1.1. pont szerinti folyamatok nem alkalmazandók egyéni vagy eseti eljárásokra;

3.1.4. a 3.1.1. pont szerinti folyamatokat a szervezetre érvényes rendelkezések szerint erre jogosult

vezetőnek kell jóváhagynia;

3.1.5. a 3.1.1. pont szerinti folyamatok előzetes tesztelésével biztosítani kell a folyamatok előre meghatározott követelmények szerinti működését;

3.1.6. a szervezetnek rendelkeznie kell információbiztonsági költség- és haszonelemzési módszertannal.

4. Az érintett szervezet biztonsági szintje 4., ha a szervezet vagy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet vagy fejleszt.

4.1. A 4. biztonsági szervezeti szint követelményei a 3. szinthez rendelt követelményeken túl:

4.1.1. az üzemeltetési vagy fejlesztési tevékenységbe épített rendszeres, előre meghatározott tesztekkel biztosítani kell az üzemeltetés vagy fejlesztés információbiztonsági intézkedéseinek hatékonyságát és megfelelőségét;

4.1.2. tesztelési eljárásban rögzítetten biztosítani kell minden szabályozási folyamat és kontroll működését az elvárt és előre meghatározott információbiztonsági követelmények szerint;

4.1.3. azonnali és eredményes, előre meghatározott biztonsági intézkedéseket kell bevezetni a feltárt vagy bekövetkezett biztonsági események kezelésére, beleértve az eseménykezelő központok, a beszállítók vagy egyéb megbízható forrás jelzése alapján lehetséges vagy bekövetkezett biztonsági esemény kezelését is;

4.1.4. folyamatba épített rendszeres belső értékelés alá kell vonni az egyes információ, rendszer vagy alkalmazás biztonsága érdekében bevezetett intézkedések megfelelőségét és hatékonyságát, mely belső értékelések részben, vagy egészben történhetnek alvállalkozók vagy más, erre feljogosított, vagy a szerv felett felügyelet gyakorló szerv bevonásával;

4.1.5. a szervezet folyamatba épített belső értékelései nem helyettesíthetőek;

4.1.6. a 4.1.3. pont szerinti forrásból származó, potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást vagy biztonsági ellenőrzést kell végezni;

4.1.7. a tesztelés értékelése alapján megállapított követelményeket, - beleértve a tesztelés típusával és gyakoriságával kapcsolatos követelményeket is - dokumentálni kell, az arra jogosulttal jóvá kell hagyatni és be kell vezetni;

4.1.8. az egyedi kontroll eljárások tesztelésének gyakoriságát és mélységét ahhoz kell igazítani, hogy milyen biztonsági kockázattal jár a kontrollok nem megfelelő működése.

5. Az érintett szervezet biztonsági szintje 5., ha a szervezet vagy szervezeti egység a 4. 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 szervezet vagy szervezeti egység.

5.1. A 5. biztonsági szervezeti szint követelményei a 4. szinthez rendelt követelményeken túl:

5.1.1. biztosítani kell az információbiztonsági kontrollfolyamatoknak a szervezet alapfeladataiba történő beépítését;

5.1.2. biztosítani kell a szabályzatok, tesztelési eljárások, biztonsági folyamatok folyamatos felülvizsgálatát és továbbfejlesztését;

5.1.3. a szervezetnek rendelkeznie kell átfogó információbiztonsági programmal, amely szerves része a szervezet feladatellátásnak és biztosítja a személyi állomány biztonságtudatosságának növelését;

5.1.4. a szervezet személyi állományának rendelkeznie kell információbiztonsági operatív képességgel és a feladat elvégzéséhez szükséges szaktudással;

5.1.5. a biztonsági sérülékenységek felismerésének és kezelésének képességét a szervezet egésze tekintetében meg kell valósítani;

5.1.6. a fenyegetettségek folyamatos újraértékelésével, a kontrollfolyamatok felülvizsgálatával nyomon

kell követni információbiztonsági környezet változását;

5.1.7. az információbiztonságot érintő külső vagy belső környezeti változásokra figyelemmel további információbiztonsági alternatívákat kell meghatározni;

5.1.8. a szervezetnek ki kell alakítania az információbiztonsági képesség- és állapotmérési és értékelési módszertanát, meg kell határozni annak mutatóit és 5.1.7. pont szerinti esetben aktualizálnia kell azt.

3. melléklet a 41/2015. (VII. 15.) BM rendelethez

1. Besorolási útmutató

1.1. Általános rendelkezések

1.2. A megvalósítandó biztonsági intézkedéseket és azok megvalósításának sorrendjét a kívánt biztonsági osztály (biztonsági szint) elérésére megalkotott intézkedési tervben kell meghatározni.

1.3. A sorszám rovatban a 4. melléklet „*3. Védelmi intézkedés katalógus*”-ának az adott számhoz rendelt intézkedésének a száma került feltüntetésre.

1.4. Az adminisztratív és fizikai védelmi intézkedések tekintetében az érintett szervezet elektronikus információs rendszerének biztonsági osztályát az 1-5. számozású oszlopok jelzik.

1.5. A logikai védelmi intézkedések követelményrendszerének kialakítása során az 1. melléklet 2. pontjára figyelemmel kell eljárni, és az elektronikus információs rendszert az információbiztonsági alapelveknek (bizalmasság, sértetlenség, rendelkezésre állás) megfelelően 2-5. osztályokba besorolni. Mivel a logikai védelmi intézkedések terén az 1. biztonsági osztály nem értelmezhető, az a táblázatban nem szerepel.

1.6. Bármely oszlopban

1.6.1. „0” jelzi, hogy a vízszintes sorban szereplő védelmi intézkedés ebben a biztonsági osztályban nem kötelező;

1.6.2. „X” jelzi, hogy a vízszintes sorban szereplő védelmi intézkedés ebben a biztonsági osztályban kötelező.

2. A 4. melléklet „3. Védelmi intézkedés katalógus” alcímben meghatározott védelmi intézkedések besorolásának táblázatai:

***A)* 3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK**

	A	B	C	D	E	F	G
1.	Sorszám	Intézkedés típusa	Biztonsági osztály				
2.			1	2	3	4	5
3.	**3.1.1.**	Szervezeti szintű alapfeladatok					
4.	3.1.1.1.	Informatikai biztonsági szabályzat	X	X	X	X	X
5.	3.1.1.2.	Az elektronikus információs rendszerek biztonságáért felelős személy	X	X	X	X	X
6.	3.1.1.3.	Az intézkedési terv és mérföldkövei	0	X	X	X	X
7.	3.1.1.4.	Az elektronikus információs rendszerek nyilvántartása	X	X	X	X	X
8.	3.1.1.5.	Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	X	X	X	X	X
9.	**3.1.2.**	Kockázatelemzés					
10.	3.1.2.1.	Kockázatelemzési és kockázatkezelési eljárásrend	X	X	X	X	X
11.	3.1.2.2.	Biztonsági osztályba sorolás	X	X	X	X	X
12.	3.1.2.3.	Kockázatelemzés	X	X	X	X	X
13.	**3.1.3.**	Rendszer és szolgáltatás beszerzés					
14.	3.1.3.1.	Beszerzési eljárásrend	0	0	X	X	X
15.	3.1.3.2.	Erőforrás igény felmérés	0	0	X	X	X
16.	3.1.3.3.	Beszerzések	0	0	X	X	X
17.	3.1.3.3.2.	A védelem szempontjainak érvényesítése a beszerzés során	0	0	0	X	X
18.	3.1.3.3.3.	A védelmi intézkedések terv-, és megvalósítási dokumentációi	0	0	0	X	X
19.	3.1.3.3.4.	Funkciók - protokollok - szolgáltatások	0	0	0	X	X
20.	3.1.3.4.	Az elektronikus információs rendszerre vonatkozó dokumentáció	0	0	X	X	X
21.	3.1.3.5.	Biztonságtervezési elvek	0	0	0	X	X
22.	3.1.3.6.	Külső elektronikus információs rendszerek szolgáltatásai	0	X	X	X	X
23.	3.1.3.7.	Független értékelők	0	0	0	X	X
24.	3.1.3.8.	Folyamatos ellenőrzés	0	0	X	X	X
25.	3.1.3.8.2.	Független értékelés	0	0	0	X	X
26.	**3.1.4.**	Üzletmenet (ügymenet) folytonosság tervezése					
27.	3.1.4.1.	Üzletmenet folytonosságra vonatkozó eljárásrend	0	X	X	X	X

28.	3.1.4.2.	Üzletmenet folytonossági terv informatikai erőforrás kiesésekre	0	X	X	X	X
29.	3.1.4.2.2.	Egyeztetés	0	0	0	X	X
30.	3.1.4.2.3.	Alapfunkciók újraindítása	0	0	0	X	X
31.	3.1.4.2.4.	Kritikus rendszerelemek meghatározása	0	0	0	X	X
32.	3.1.4.2.5.	Kapacitástervezés	0	0	0	0	X
33.	3.1.4.2.6.	Összes funkció újraindítása	0	0	0	0	X
34.	3.1.4.2.7.	Alapfeladatok és funkciók folyamatossága	0	0	0	0	X
35.	3.1.4.3.	A folyamatos működésre felkészítő képzés	0	0	X	X	X
36.	3.1.4.3.2.	Szimuláció	0	0	0	0	X
37.	3.1.4.4.	Az üzletmenet folytonossági terv tesztelése	0	0	0	X	X
38.	3.1.4.4.2.	Koordináció	0	0	0	X	X
39.	3.1.4.4.3.	Tesztelés a tartalék feldolgozási helyszínen	0	0	0	X	X
40.	3.1.4.5.	Biztonsági tárolási helyszín	0	0	0	X	X
41.	3.1.4.5.2.	A tartalék feldolgozási helyszín elkülönítése	0	0	0	X	X
42.	3.1.4.5.3.	Üzletmenet folytonosság elérhetőség	0	0	0	X	X
43.	3.1.4.5.4.	Üzletmenet folytonosság helyreállítás	0	0	0	0	X
44.	3.1.4.6.	Tartalék feldolgozási helyszín	0	0	0	X	X
45.	3.1.4.6.2.	Elkülönítés	0	0	0	0	X
46.	3.1.4.6.3.	Elérhetőség	0	0	0	0	X
47.	3.1.4.6.4.	Szolgáltatások priorálása a tartalék feldolgozási helyszínen	0	0	0	0	X
48.	3.1.4.6.5.	Előkészület a működés megindítására	0	0	0	0	X
49.	3.1.4.7.	Infokommunikációs szolgáltatások	0	0	0	X	X
50.	3.1.4.7.2.	Szolgáltatás-prioritási rendelkezések	0	0	0	X	X
51.	3.1.4.7.3.	Közös hibalehetőségek kizárása	0	0	0	X	X
52.	3.1.4.8.	Az elektronikus információs rendszer mentései	0	X	X	X	X
53.	3.1.4.8.2.	Megbízhatósági és sértetlenségi teszt	0	0	0	X	X
54.	3.1.4.8.3.	Helyreállítási teszt	0	0	0	0	X
55.	3.1.4.8.4.	Kritikus információk elkülönítése	0	0	0	0	X
56.	3.1.4.8.5.	Alternatív tárolási helyszín	0	0	0	0	X
57.	3.1.4.9.	Az elektronikus információs rendszer helyreállítása és újraindítása	0	X	X	X	X
58.	3.1.4.9.2.	Tranzakciók helyreállítása	0	0	0	X	X
59.	3.1.4.9.3.	Helyreállítási idő	0	0	0	0	X
60.	**3.1.5.**	A biztonsági események kezelése					
61.	3.1.5.1.	Biztonsági eseménykezelési eljárásrend	0	0	X	X	X
62.	3.1.5. 2.	Automatikus eseménykezelés	0	0	0	0	X
63.	3.1.5. 3.	Információ korreláció	0	0	0	0	X
64.	3.1.5.4.	A biztonsági események figyelése	0	0	X	X	X
65.	3.1.5.5.	Automatikus nyomonkövetés, adatgyűjtés és vizsgálat	0	0	0	0	X
66.	3.1.5.6.	A biztonsági események jelentése	0	0	X	X	X
67.	3.1.5.6.2	Automatizált jelentés	0	0	0	X	X
68.	3.1.5.7.	Segítségnyújtás a biztonsági események kezeléséhez	0	0	X	X	X
69.	3.1.5.7.2.	Automatizált támogatás	0	0	0	X	X
70.	3.1.5.8.	Biztonsági eseménykezelési terv	0	0	X	X	X
71.	3.1.5.9.	Képzés a biztonsági események kezelésére	0	0	X	X	X
72.	3.1.5.9.2.	Szimuláció	0	0	0	0	X
73.	3.1.5.9.3.	Automatizált képzési környezet	0	0	0	0	X
74.	3.1.5.9.4	A biztonsági események kezelésének tesztelése	0	0	0	X	X
75.	3.1.5.9.4.2.	Egyeztetés	0	0	0	X	X
76.	**3.1.6.**	Emberi tényezőket figyelembe vevő - személy - biztonság					
77.	3.1.6.1.	Személybiztonsági eljárásrend	0	0	X	X	X
78.	3.1.6.2.	Munkakörök, feladatok biztonsági szempontú besorolása	0	0	X	X	X
79.	3.1.6.3.	A személyek ellenőrzése	0	0	X	X	X
80.	3.1.6.4.	Eljárás a jogviszony megszűnésekor	X	X	X	X	X
81.	3.1.6.5.	Az áthelyezések, átirányítások és kirendelések kezelése	0	0	X	X	X
82.	3.1.6.6.	Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények	0	0	X	X	X
83.	3.1.6.7.	Fegyelmi intézkedések	X	X	X	X	X
84.	3.1.6.8	Belső egyeztetés	0	0	X	X	X
85.	3.1.6.9.	Viselkedési szabályok az interneten	X	X	X	X	X
86.	**3.1.7.**	Tudatosság és képzés					
87.	3.1.7.1.	Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel	0	0	X	X	X
88.	3.1.7.2.	Képzési eljárásrend	X	X	X	X	X
89.	3.1.7.3.	Biztonság tudatosság képzés	X	X	X	X	X
90.	3.1.7.4.	Belső fenyegetés	0	0	0	X	X
91.	3.1.7.5.	Szerepkör, vagy feladat alapú biztonsági képzés	0	0	X	X	X
92.	3.1.7.6.	A biztonsági képzésre vonatkozó dokumentációk	0	0	X	X	X

***B)* 3.2. FIZIKAI VÉDELMI INTÉZKEDÉSEK**

	A	B	C	D	E	F	G
1.	**Sorszám**	Intézkedés típusa	Biztonsági osztály				
2.			**1**	2	3	4	5
3.	3.2.1.2.	Fizikai védelmi eljárásrend	0	X	X	X	X

4.	3.2.1.3.	Fizikai belépési engedélyek	0	X	X	X	X
5.	3.2.1.4.	A fizikai belépés ellenőrzése	0	X	X	X	X
6.	3.2.1.4.2.	Hozzáférés az információs rendszerhez	0	0	0	0	X
7.	3.2.1.5.	Hozzáférés az adatátviteli eszközökhöz és csatornákhoz	0	0	0	X	X
8.	3.2.1.6.	A kimeneti eszközök hozzáférés ellenőrzése	0	0	0	X	X
9.	3.2.1.7.	A fizikai hozzáférések felügyelete	0	0	X	X	X
10.	3.2.1.7.2.	Behatolás riasztás, felügyeleti berendezések	0	0	0	X	X
11.	3.2.1.7.3.	Az elektronikus információs rendszerekhez való hozzáférés felügyelete	0	0	0	0	X
12.	3.2.1.8.	A látogatók ellenőrzése	0	0	X	X	X
13.	3.2.1.8.2.	Automatizált látogatói információkezelés	0	0	0	0	X
14.	3.2.1.9.	Áramelláto berendezések és kábelezés	0	0	0	X	X
15.	3.2.1.9.1.	Tartalék áramellátás	0	0	0	X	X
16.	3.2.1.9.2.	Hosszú távú tartalék áramellátás a minimálisan elvárt működési képességhez	0	0	0	0	X
17.	3.2.1.10.	Vészkikapcsolás	0	0	0	X	X
18.	3.2.1.11.	Vészvilágítás	0	0	X	X	X
19.	3.2.1.12.	Tűzvédelem	0	0	X	X	X
20.	3.2.1.12.2.	Automatikus tűzelfojtás	0	0	0	X	X
21.	3.2.1.12.3.	Észlelő berendezések, rendszerek	0	0	0	0	X
22.	3.2.1.12.4.	Tűzelfojtó berendezések, rendszerek	0	0	0	0	X
23.	3.2.1.13.	Hőmérséklet és páratartalom ellenőrzés	0	0	X	X	X
24.	3.2.1.14.	Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	0	0	X	X	X
25.	3.2.1.14.2.	Automatizált védelem	0	0	0	0	X
26.	3.2.1.15.	Be- és kiszállítás	0	0	X	X	X
27.	3.2.1.16.	Az elektronikus információs rendszer elemeinek elhelyezése	0	0	0	X	X
28.	3.2.1.17.	Ellenőrzés	0	0	0	X	X
29.	3.2.1.18.	Szállítási felügyelet	0	0	0	0	X
30.	3.2.1.19.	Karbantartók	0	0	X	X	X
31.	3.2.1.19.2.	Karbantartás fokozott biztonsági intézkedésekkel	0	0	0	0	X
32.	3.2.1.19.3.	Időben történő javítás	0	0	0	X	X

***C)* 3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1.	**Sorszám**	Intézkedés típusa	Alapelvek											
2.			**Bizalmasság**				**Sértetlenség**				**Rendelkezésre állás**			
3.			**Biztonsági osztályok**											
4.			**2**	3	4	5	2	3	4	5	2	3	4	5
5.	**3.3.1.**	Általános védelmi intézkedések												
6.	3.3.1.3.	Az elektronikus információs rendszer kapcsolódásai	0	X	X	X	0	X	X	X	0	X	X	X
7.	3.3.1.3.2.	Belső rendszer kapcsolatok	0	X	X	X	0	X	X	X	0	X	X	X
8.	3.3.1.3.3.	Külső kapcsolódásokra vonatkozó korlátozások	0	X	X	X	0	X	X	X	0	X	X	X
9.	3.3.1.4.	Személybiztonság	X	X	X	X	X	X	X	X	X	X	X	X
10.	**3.3.2.**	Tervezés												
11.	3.3.2.1.	Biztonságtervezési szabályzat	0	0	X	X	0	0	X	X	0	0	X	X
12.	3.3.2.2.	Rendszerbiztonsági terv	X	X	X	X	X	X	X	X	X	X	X	X
13.	3.3.2.3.	Cselekvési terv	X	X	X	X	X	X	X	X	0	0	0	0
14.	3.3.2.4.	Személyi biztonság	X	X	X	X	0	0	0	0	0	0	0	0
15.	3.3.2.5.	Információbiztonsági architektúra leírás	0	0	X	X	0	0	0	0	0	0	0	0
16.	**3.3.3.**	Rendszer és szolgáltatás beszerzés												
17.	3.3.3.2.	A rendszer fejlesztési életciklusa	X	X	X	X	0	0	0	0	0	0	0	0
18.	3.3.3.3.	Funkciók, portok, protokollok, szolgáltatások	0	X	X	X	0	X	X	X	0	X	X	X
19.	3.3.3.4.	Fejlesztői változáskövetés	0	0	X	X	0	0	X	X	0	0	X	X
20.	3.3.3.5.	Fejlesztői biztonsági tesztelés	0	0	X	X	0	0	X	X	0	0	X	X
21.	3.3.3.6	Fejlesztési folyamat, szabványok és eszközök	0	0	0	X	0	0	0	X	0	0	0	X
22.	3.3.3.7.	Fejlesztői oktatás	0	0	0	X	0	0	0	0	0	0	0	0
23.	3.3.3.8.	Fejlesztői biztonsági architektúra és tervezés	0	0	0	X	0	0	0	X	0	0	0	X
24.	**3.3.4.**	Biztonsági elemzés												
25.	3.3.4.1.	Biztonságelemzési eljárásrend	0	X	X	X	0	X	X	X	0	X	X	X
26.	3.3.4.2.	Biztonsági értékelések	0	X	X	X	0	X	X	X	0	X	X	X
27.	3.3.4.3.	Speciális értékelés	0	0	X	X	0	0	X	X	0	0	X	X
28.	3.3.4.4.	A biztonsági teljesítmény mérése	0	X	X	X	0	X	X	X	0	X	X	X
29.	**3.3.5.**	Tesztelés, képzés és felügyelet												
30.	3.3.5.1.1.	Tesztelési, képzési és felügyeleti eljárások	0	X	X	X	0	X	X	X	0	X	X	X
31.	3.3.5.2.	A biztonsági teljesítmény mérése	0	X	X	X	0	X	X	X	0	X	X	X
32.	3.3.5.3.	Sérülékenység teszt	0	X	X	X	0	X	X	X	0	X	X	X
33.	3.3.5.3.2.	Frissítési képesség	0	X	X	X	0	0	0	0	0	0	0	0
34.	3.3.5.3.3.	Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően	0	X	X	X	0	0	0	0	0	0	0	0
35.	3.3.5.3.4.	Privilegizált hozzáférés	0	X	X	X	0	X	X	X	0	X	X	X
36.	3.3.5.3.5.	Felfedhető információk	0	X	X	X	0	X	X	X	0	X	X	X
37.	**3.3.6.**	Konfigurációkezelés												
38.	3.3.6.1.	Konfigurációkezelési eljárásrend	X	X	X	X	X	X	X	X	X	X	X	X
39.	3.3.6.2.	Alap konfiguráció	X	X	X	X	X	X	X	X	X	X	X	X
40.	3.3.6.2.2.	Áttekintések és frissítések	0	0	X	X	0	0	X	X	0	0	X	X

41.	3.3.6.2.3.	Korábbi konfigurációk megőrzése	0	0	X	X	0	0	X	X	0	0	X	X
42.	3.3.6.2.4.	Magas kockázatú területek konfigurálása	0	0	X	X	0	0	X	X	0	0	X	X
43.	3.3.6.2.5.	Automatikus támogatás	0	0	0	X	0	0	0	X	0	0	0	X
44.	3.3.6.3.	A konfigurációváltozások felügyelete (változáskezelés)	0	X	X	X	0	X	X	X	0	X	X	X
45.	3.3.6.3.2.	Előzetes tesztelés és megerősítés	0	0	X	X	0	0	X	X	0	X	X	X
46.	3.3.6.3.3.	Automatikus támogatás	0	0	0	X	0	0	0	X	0	0	0	X
47.	3.3.6.4.	Biztonsági hatásvizsgálat	0	X	X	X	0	X	X	X	0	X	X	X
48.	3.3.6.4.2.	Elkülönített teszt környezet	0	0	0	X	0	0	0	X	0	0	0	X
49.	3.3.6.5.	A változtatásokra vonatkozó hozzáférés korlátozások	0	0	0	0	0	0	X	X	0	0	0	0
50.	3.3.6.5.2.	Automatikus támogatás	0	0	0	0	0	0	0	X	0	0	0	0
51.	3.3.6.5.3.	Felülvizsgálat	0	0	0	0	0	0	0	X	0	0	0	0
52.	3.3.6.5.4.	Aláírt elemek	0	0	0	0	0	0	0	X	0	0	0	0
53.	3.3.6.6.	Konfigurációs beállítások	0	X	X	X	0	X	X	X	0	X	X	X
54.	3.3.6.6.2.	Automatikus támogatás	0	0	0	X	0	0	0	X	0	0	0	X
55.	3.3.6.6.3.	Reagálás jogosulatlan változásokra	0	0	0	X	0	0	0	X	0	0	0	X
56.	3.3.6.7.	Legszűkebb funkcionalitás	0	X	X	X	0	X	X	X	0	X	X	X
57.	3.3.6.7.2.	Rendszeres felülvizsgálat	0	0	X	X	0	0	X	X	0	0	X	X
58.	3.3.6.7.3.	Nem futtatható szoftverek	0	0	X	X	0	0	X	X	0	0	X	X
59.	3.3.6.7.4.	Futtatható szoftverek	0	0	0	X	0	0	0	X	0	0	0	X
60.	3.3.6.8.	Elektronikus információs rendszerelem leltár	X	X	X	X	X	X	X	X	X	X	X	X
61.	3.3.6.8.2.	Frissítés	0	0	X	X	0	0	X	X	0	0	X	X
62.	3.3.6.8.3.	Jogosulatlan elemek automatikus észlelése	0	0	0	X	0	0	0	X	0	0	X	X
63.	3.3.6.8.4.	Duplikálás elleni védelem	0	0	0	X	0	0	0	X	0	0	X	X
64.	3.3.6.8.5.	Automatikus támogatás	0	0	0	X	0	0	0	X	0	0	0	X
65.	3.3.6.8.6.	Naplózás	0	0	0	X	0	0	0	X	0	0	0	X
66.	3.3.6.9.	Konfigurációkezelési terv	0	0	X	X	0	0	X	X	0	0	X	X
67.	3.3.6.10.	A szoftver használat korlátozásai	X	X	X	X	X	X	X	X	X	X	X	X
68.	3.3.6.11.	A felhasználó által telepített szoftverek	X	X	X	X	X	X	X	X	X	X	X	X
69.	**3.3.7.**	Karbantartás												
70.	3.3.7.1.	Rendszer karbantartási eljárásrend	0	0	0	0	X	X	X	X	X	X	X	X
71.	3.3.7.2.	Rendszeres karbantartás	0	0	0	0	X	X	X	X	X	X	X	X
72.	3.3.7.2.2.	Automatikus támogatás	0	0	0	0	0	0	0	X	0	0	0	X
73.	3.3.7.3.	Karbantartási eszközök	0	0	0	0	0	0	X	X	0	0	X	X
74.	3.3.7.3.2.	Adathordozó ellenőrzés	0	0	0	0	0	0	X	X	0	0	X	X
75.	3.3.7.4.	Távoli karbantartás	0	0	X	X	0	0	X	X	0	0	X	X
76.	3.3.7.4.2.	Dokumentálás	0	0	0	X	0	0	0	X	0	0	0	X
77.	3.3.7.4.3.	Összehasonlítható biztonság	0	0	0	X	0	0	0	X	0	0	0	X
78.	**3.3.8.**	Adathordozók védelme												
79.	3.3.8.1.	Adathordozók védelmére vonatkozó eljárásrend	X	X	X	X	X	X	X	X	X	X	X	X
80.	3.3.8.2.	Hozzáférés az adathordozókhoz	X	X	X	X	X	X	X	X	X	X	X	X
81.	3.3.8.3.	Adathordozók címkézése	0	0	X	X	0	0	0	0	0	0	0	0
82.	3.3.8.4.	Adathordozók tárolása	0	0	X	X	0	0	0	0	0	0	0	0
83.	3.3.8.5.	Adathordozók szállítása	0	0	X	X	0	0	X	X	0	0	X	X
84.	3.3.8.5.2.	Kriptográfiai védelem	0	0	X	X	0	0	X	X	0	0	0	0
85.	3.3.8.6.	Adathordozók törlése	X	X	X	X	0	0	0	0	0	0	0	0
86.	3.3.8.6.2.	Ellenőrzés	0	0	0	X	0	0	0	0	0	0	0	0
87.	3.3.8.6.3.	Tesztelés	0	0	0	X	0	0	0	0	0	0	0	0
88.	3.3.8.6.4.	Törlés megsemmisítés nélkül	0	0	0	X	0	0	0	0	0	0	0	0
89.	3.3.8.7.	Adathordozók használata	X	X	X	X	X	X	X	X	X	X	X	X
90.	3.3.8.7.2.	Ismeretlen tulajdonos	0	0	X	X	0	0	X	X	0	0	X	X
91.	**3.3.9.**	Azonosítás és hitelesítés												
92.	3.3.9.1.	Azonosítási és hitelesítési eljárásrend	X	X	X	X	X	X	X	X	X	X	X	X
93.	3.3.9.2.	Azonosítás és hitelesítés	X	X	X	X	X	X	X	X	X	X	X	X
94.	3.3.9.2.2.	Hálózati hozzáférés privilegizált fiókokhoz	0	X	X	X	0	0	X	X	0	0	X	X
95.	3.3.9.2.3.	Hálózati hozzáférés nem privilegizált fiókokhoz	0	0	X	X	0	0	X	X	0	0	X	X
96.	3.3.9.2.4.	Helyi hozzáférés privilegizált fiókokhoz	0	0	X	X	0	0	X	X	0	0	X	X
97.	3.3.9.2.5.	Visszajátszás-védelem	0	0	X	X	0	0	X	X	0	0	X	X
98.	3.3.9.2.6.	Távoli hozzáférés - külön eszköz	0	0	X	X	0	0	X	X	0	0	X	X
99.	3.3.9.2.7.	Helyi hozzáférés nem privilegizált fiókokhoz	0	0	0	X	0	0	0	X	0	0	X	X
100.	3.3.9.2.8.	Visszajátszás ellen védett hálózati hozzáférés nem privilegizált fiókokhoz	0	0	0	X	0	0	0	X	0	0	X	X
101.	3.3.9.3.	Eszközök azonosítása és hitelesítése	0	0	X	X	0	0	X	X	0	0	X	X
102.	3.3.9.4.	Azonosító kezelés	X	X	X	X	X	X	X	X	X	X	X	X
103.	3.3.9.5.	A hitelesítésre szolgáló eszközök kezelése	X	X	X	X	X	X	X	X	X	X	X	X
104.	3.3.9.5.2.	Jelszó (tudás) alapú hitelesítés	0	0	X	X	0	0	X	X	0	0	X	X
105.	3.3.9.5.3.	Birtoklás alapú hitelesítés	0	0	X	X	0	0	X	X	0	0	X	X
106.	3.3.9.5.4.	Tulajdonság alapú hitelesítés	0	0	X	X	0	0	X	X	0	0	X	X
107.	3.3.9.5.5.	Személyes vagy megbízható harmadik fél általi regisztráció	0	0	X	X	0	0	X	X	0	0	X	X
108.	3.3.9.6.	A hitelesítésre szolgáló eszköz visszacsatolása	X	X	X	X	X	X	X	X	X	X	X	X
109.	3.3.9.7.	Hitelesítés kriptográfiai modul esetén	0	X	X	X	0	X	X	X	0	X	X	X
110.	3.3.9.8.	Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	X	X	X	X	X	X	X	X	X	X	X	X
111.	3.3.9.8.2.	Hitelesítés szolgáltatók tanúsítványának elfogadása	0	X	X	X	X	X	X	X	X	X	X	X
112.	**3.3.10.**	Hozzáférés ellenőrzése												

113.	3.3.10.1.	Hozzáférés ellenőrzési eljárásrend	X	X	X	X	X	X	X	X	X	X	X	X
114.	3.3.10.2.	Felhasználói fiókok kezelése	X	X	X	X	X	X	X	X	X	X	X	X
115.	3.3.10.2.2.	Automatikus kezelés	0	0	X	X	0	0	X	X	0	0	X	X
116.	3.3.10.2.3.	Ideiglenes fiókok eltávolítása	0	0	X	X	0	0	X	X	0	0	X	X
117.	3.3.10.2.4.	Inaktív fiókok letiltása	0	0	X	X	0	0	X	X	0	0	X	X
118.	3.3.10.2.5.	Automatikus naplózás	0	0	X	X	0	0	0	X	0	0	X	X
119.	3.3.10.2.6.	Kiléptetés	0	0	0	X	0	0	0	X	0	0	0	X
120.	3.3.10.2.7.	Szokatlan használat	0	0	0	X	0	0	0	X	0	0	0	X
121.	3.3.10.2.8.	Letiltás	0	0	0	X	0	0	0	X	0	0	0	X
122.	3.3.10.3.	Hozzáférés ellenőrzés érvényesítése	X	X	X	X	X	X	X	X	X	X	X	X
123.	3.3.10.4.	Információáramlás ellenőrzés érvényesítése	0	0	X	X	0	0	X	X	0	0	X	X
124.	3.3.10.5.	A felelősségek szétválasztása	0	0	X	X	0	0	X	X	0	0	X	X
125.	3.3.10.6.	Legkisebb jogosultság elve	0	0	X	X	0	0	X	X	0	0	X	X
126.	3.3.10.6.2.	Jogosult hozzáférés a biztonsági funkciókhoz	0	0	X	X	0	0	X	X	0	0	X	X
127.	3.3.10.6.3.	Nem privilegizált hozzáférés a biztonsági funkciókhoz	0	0	X	X	0	0	X	X	0	0	X	X
128.	3.3.10.6.4.	Privilegizált fiókok	0	0	X	X	0	0	X	X	0	0	X	X
129.	3.3.10.6.5.	Privilegizált funkciók használatának naplózása	0	0	X	X	0	0	X	X	0	0	X	X
130.	3.3.10.6.6.	Privilegizált funkciók tiltása nem privilegizált felhasználóknak	0	0	X	X	0	0	X	X	0	0	X	X
131.	3.3.10.6.7.	Hálózati hozzáférés a privilegizált parancsokhoz	0	0	0	X	0	0	0	X	0	0	0	X
132.	3.3.10.7.	Sikertelen bejelentkezési kísérletek	0	X	X	X	0	X	X	X	0	X	X	X
133.	3.3.10.8.	A rendszerhasználat jelzése	0	X	X	X	0	X	X	X	0	X	X	X
134.	3.3.10.9.	Egyidejű munkaszakasz kezelés	0	0	0	X	0	0	0	X	0	0	0	X
135.	3.3.10.10.	A munkaszakasz zárolása	0	0	X	X	0	0	X	X	0	0	X	X
136.	3.3.10.10.2.	Képernyőtakarás	0	0	X	X	0	0	X	X	0	0	X	X
137.	3.3.10.11.	A munkaszakasz lezárása	0	0	X	X	0	0	X	X	0	0	X	X
138.	3.3.10.12.	Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	X	X	X	X	X	X	X	X	X	X	X	X
139.	3.3.10.13.	Távoli hozzáférés	0	X	X	X	0	X	X	X	0	X	X	X
140.	3.3.10.13.2.	Ellenőrzés	0	0	X	X	0	0	X	X	0	0	X	X
141.	3.3.10.13.3.	Titkosítás	0	0	X	X	0	0	X	X	0	0	X	X
142.	3.3.10.13.4.	Hozzáférés ellenőrzési pontok	0	0	X	X	0	0	X	X	0	0	X	X
143.	3.3.10.13.5.	Privilegizált parancsok elérése	0	0	X	X	0	0	X	X	0	0	X	X
144.	3.3.10.14.	Vezeték nélküli hozzáférés	0	X	X	X	0	X	X	X	0	X	X	X
145.	3.3.10.14.2.	Hitelesítés és titkosítás	0	0	0	X	0	0	0	X	0	0	0	X
146.	3.3.10.14.3.	Felhasználó konfigurálás tiltása	0	0	0	X	0	0	0	X	0	0	0	X
147.	3.3.10.14.4.	Antennák	0	0	0	X	0	0	0	X	0	0	0	X
148.	3.3.10.15.	Mobil eszközök hozzáférés ellenőrzése	0	X	X	X	0	X	X	X	0	X	X	X
149.	3.3.10.15.2.	Titkosítás	0	0	X	X	0	0	X	X	0	0	0	0
150.	3.3.10.16.	Külső elektronikus információs rendszerek használata	X	X	X	X	X	X	X	X	X	X	X	X
151.	3.3.10.16.2.	Korlátozott használat	0	0	X	X	0	0	X	X	0	0	X	X
152.	3.3.10.16.3.	Hordozható adattároló eszközök	0	0	X	X	0	0	X	X	0	0	X	X
153.	3.3.10.17.	Információ megosztás	0	0	X	X	0	0	0	0	0	0	0	0
154.	3.3.10.18.	Nyilvánosan elérhető tartalom	X	X	X	X	X	X	X	X	X	X	X	X
155.	**3.3.11.**	Rendszer és információ sértetlenség												
156.	3.3.11.2.	Rendszer és információ sértetlenségre vonatkozó eljárásrend	0	0	0	0	X	X	X	X	0	0	0	0
157.	3.3.11.3.	Hibajavítás	0	0	0	0	X	X	X	X	0	0	0	0
158.	3.3.11.3.2.	Automatizált hibajavítási állapot	0	0	0	0	0	0	X	X	0	0	0	0
159.	3.3.11.3.3.	Központi kezelés	0	0	0	0	0	0	0	X	0	0	0	0
160.	3.3.11.4.	Kártékony kódok elleni védelem	X	X	X	X	X	X	X	X	X	X	X	X
161.	3.3.11.4.2.	Központi kezelés	0	0	X	X	0	0	X	X	0	0	X	X
162.	3.3.11.4.3.	Automatikus frissítés	0	0	X	X	0	0	X	X	0	0	X	X
163.	3.3.11.5.	Az elektronikus információs rendszer felügyelete	X	X	X	X	X	X	X	X	X	X	X	X
164.	3.3.11.5.2.	Automatizálás	0	0	X	X	0	0	X	X	0	0	X	X
165.	3.3.11.5.3.	Felügyelet	0	0	X	X	0	0	X	X	0	0	X	X
166.	3.3.11.5.4.	Riasztás	0	0	X	X	0	0	X	X	0	0	X	X
167.	3.3.11.6.	Biztonsági riasztások és tájékoztatások	0	X	X	X	0	X	X	X	0	X	X	X
168.	3.3.11.6.2.	Automatikus riasztások	0	0	0	X	0	0	0	X	0	0	0	X
169.	3.3.11.7.	A biztonsági funkcionalitás ellenőrzése	0	0	0	X	0	0	0	X	0	0	0	0
170.	3.3.11.8.	Szoftver és információ sértetlenség	0	0	X	X	0	0	X	X	0	0	X	X
171.	3.3.11.8.2.	Sértetlenség ellenőrzés	0	0	0	X	0	0	0	X	0	0	0	X
172.	3.3.11.8.3.	Észlelés és reagálás	0	0	0	X	0	0	0	X	0	0	0	X
173.	3.3.11.8.4.	Automatikus értesítés	0	0	0	X	0	0	0	X	0	0	0	X
174.	3.3.11.8.5.	Automatikus reagálás	0	0	0	X	0	0	0	X	0	0	0	X
175.	3.3.11.8.6.	Végrehajtható kód	0	0	0	X	0	0	0	X	0	0	0	X
176.	3.3.11.9.	Kéretlen üzenetek elleni védelem	0	0	0	0	0	0	X	X	0	0	0	0
177.	3.3.11.9.2.	Központi kezelés	0	0	0	0	0	0	X	X	0	0	0	0
178.	3.3.11.9.3.	Frissítés	0	0	0	0	0	0	X	X	0	0	0	0
179.	3.3.11.10.	Bemeneti információ ellenőrzés	0	0	0	0	0	0	X	X	0	0	0	0
180.	3.3.11.11.	Hibakezelés	0	0	0	0	0	0	X	X	0	0	0	0
181.	3.3.11.12.	A kimeneti információ kezelése és megőrzése	X	X	X	X	X	X	X	X	0	0	0	0
182.	3.3.11.13.	Memória védelem	0	0	X	X	0	0	X	X	0	0	X	X
183.	**3.3.12.**	Naplózás és elszámoltathatóság												
184.	3.3.12.1.	Naplózási eljárásrend	X	X	X	X	X	X	X	X	X	X	X	X

185.	3.3.12.2.	Naplózható események	X	X	X	X	X	X	X	X	X	X	X	X
186.	3.3.12.2.2.	Felülvizsgálat	0	0	0	X	0	0	0	X	0	0	0	X
187.	3.3.12.3.	Naplóbejegyzések tartalma	X	X	X	X	X	X	X	X	X	X	X	X
188.	3.3.12.3.2.	Kiegészítő információk	0	0	X	X	0	0	X	X	0	0	X	X
189.	3.3.12.3.3.	Központi kezelés	0	0	0	X	0	0	0	X	0	0	0	X
190.	3.3.12.4.	Napló tárkapacitás	0	X	X	X	0	X	X	X	0	X	X	X
191.	3.3.12.5.	Naplózási hiba kezelése	0	X	X	X	0	X	X	X	0	X	X	X
192.	3.3.12.5.2.	Naplózási tárhely ellenőrzés	0	0	0	X	0	0	0	X	0	0	0	X
193.	3.3.12.5.3.	Valósidejű riasztás	0	0	0	X	0	0	0	X	0	0	0	X
194.	3.3.12.6.	Naplóvizsgálat és jelentéskészítés	0	X	X	X	0	X	X	X	0	X	X	X
195.	3.3.12.6.2.	Folyamatba illesztés	0	0	0	X	0	0	0	X	0	0	X	X
196.	3.3.12.6.3.	Összegzés	0	0	0	X	0	0	0	X	0	0	X	X
197.	3.3.12.6.4.	Felügyeleti képességek integrálása	0	0	0	X	0	0	0	X	0	0	0	X
198.	3.3.12.6.5.	Összekapcsolás a fizikai hozzáférési információkkal	0	0	0	X	0	0	0	X	0	0	0	X
199.	3.3.12.7.	Naplócsökkentés és jelentéskészítés	0	0	X	X	0	0	X	X	0	0	X	X
200.	3.3.12.7.2.	Automatikus feldolgozás	0	0	X	X	0	0	X	X	0	0	X	X
201.	3.3.12.8.	Időbélyegek	X	X	X	X	X	X	X	X	X	X	X	X
202.	3.3.12.8.2.	Szinkronizálás	0	0	X	X	0	0	X	X	0	0	X	X
203.	3.3.12.9.	A naplóinformációk védelme	X	X	X	X	X	X	X	X	X	X	X	X
204.	3.3.12.9.2.	Hozzáférés korlátozás	0	0	0	0	0	0	0	X	0	0	X	X
205.	3.3.12.9.3.	Fizikailag elkülönített mentés	0	0	0	0	0	0	0	X	0	0	0	X
206.	3.3.12.9.4.	Kriptográfiai védelem	0	0	0	0	0	0	0	X	0	0	0	0
207.	3.3.12.10.	Letagadhatatlanság	0	0	0	X	0	0	0	X	0	0	0	X
208.	3.3.12.11.	A naplóbejegyzések megőrzése	X	X	X	X	X	X	X	X	X	X	X	X
209.	3.3.12.12.	Naplógenerálás	X	X	X	X	X	X	X	X	X	X	X	X
210.	3.3.12.12.2.	Rendszerszintű időalap napló	0	0	0	X	0	0	0	X	0	0	0	X
211.	3.3.12.12.3.	Változtatások	0	0	0	X	0	0	0	X	0	0	0	X
212.	**3.3.13.**	Rendszer- és kommunikáció védelem												
213.	3.3.13.1.	Rendszer- és kommunikáció védelmi eljárásrend	X	X	X	X	X	X	X	X	X	X	X	X
214.	3.3.13.2.	Alkalmazás szétválasztás	0	0	X	X	0	0	X	X	0	0	X	X
215.	3.3.13.3.	Biztonsági funkciók elkülönítése	0	0	0	X	0	0	0	X	0	0	0	X
216.	3.3.13.4.	Információmaradványok	0	0	X	X	0	0	0	0	0	0	0	0
217.	3.3.13.5.	Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem	0	0	0	0	0	0	0	0	0	X	X	X
218.	3.3.13.6.	A határok védelme	X	X	X	X	X	X	X	X	X	X	X	X
219.	3.3.13.6.2.	Hozzáférési pontok	0	0	0	X	0	0	0	X	0	0	X	X
220.	3.3.13.6.3.	Külső kommunikációs szolgáltatások	0	0	0	X	0	0	0	X	0	0	X	X
221.	3.3.13.6.4.	Alapeseti visszautasítás	0	0	0	X	0	0	0	X	0	0	X	X
222.	3.3.13.6.5.	Távoli készülékek megosztott csatornahasználatának tiltása	0	0	0	X	0	0	0	X	0	0	X	X
223.	3.3.13.6.6.	Hitelesített proxy kiszolgálók	0	0	0	X	0	0	0	X	0	0	0	X
224.	3.3.13.6.7.	Biztonsági hibaállapot	0	0	0	X	0	0	0	X	0	0	0	X
225.	3.3.13.6.8.	Rendszerelemek elkülönítése	0	0	0	X	0	0	0	X	0	0	0	X
226.	3.3.13.7.	Az adatátvitel bizalmassága	0	0	X	X	0	0	0	0	0	0	0	0
227.	3.3.13.7.2.	Kriptográfiai vagy egyéb védelem	0	0	X	X	0	0	0	0	0	0	0	0
228.	3.3.13.8.	Az adatátvitel sértetlensége	0	0	0	0	0	0	X	X	0	0	0	0
229.	3.3.13.8.2.	Kriptográfiai vagy egyéb védelem	0	0	0	0	0	0	X	X	0	0	0	0
230.	3.3.13.9.	A hálózati kapcsolat megszakítása	0	0	0	0	0	0	0	0	0	0	X	X
231.	3.3.13.10.	Kriptográfiai kulcs előállítása és kezelése	X	X	X	X	X	X	X	X	X	X	X	X
232.	3.3.13.10.2.	Rendelkezésre állás	0	0	0	X	0	0	0	X	0	0	0	X
233.	3.3.13.11.	Kriptográfiai védelem	X	X	X	X	X	X	X	X	0	0	0	0
234.	3.3.13.12.	Együttműködésen alapuló számítástechnikai eszközök	X	X	X	X	0	0	0	0	0	0	0	0
235.	3.3.13.13.	Nyilvános kulcsú infrastruktúra tanúsítványok	0	0	X	X	0	0	X	X	0	0	0	0
236.	3.3.13.14.	Mobilkód korlátozása	0	0	X	X	0	0	X	X	0	0	0	0
237.	3.3.13.15.	Elektronikus Információs rendszeren keresztüli hangátvitel (úgynevezett VoIP)	0	0	X	X	0	0	0	0	0	0	0	0
238.	3.3.13.16.	Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás)	0	0	0	0	0	X	X	X	0	0	0	0
239.	3.3.13.17.	Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás)	0	0	0	0	0	X	X	X	0	0	0	0
240.	3.3.13.18.	Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	0	0	0	0	0	X	X	X	0	0	0	0
241.	3.3.13.19.	Munkaszakasz hitelessége	0	0	0	0	0	0	X	X	0	0	0	0
242.	3.3.13.20.	Hibát követő ismert állapot	0	0	0	X	0	0	0	X	0	0	0	X
243.	3.3.13.21.	A maradvány információ védelme	0	0	X	X	0	0	X	X	0	0	0	0
244.	3.3.13.22.	A folyamatok elkülönítése	X	X	X	X	X	X	X	X	0	0	0	0

4. melléklet a 41/2015. (VII. 15.) BM rendelethez

AZ ADMINISZTRATÍV, FIZIKAI ÉS LOGIKAI BIZTONSÁGI KÖVETELMÉNYEK

1. ELTÉRÉSEK

1.1. Általános követelmények

Az érintett szervezetnek az alábbi lehetséges eltérésekkel és helyettesítő intézkedésekkel lehet teljesítenie a 3. pont szerinti védelmi intézkedés katalógusban meghatározott minimális követelményeket, a rendszerre meghatározott biztonsági kockázati szintnek megfelelő intézkedések kiválasztásával, amellett, hogy az érintett szervezetre érvényes minden kötelezettséget figyelembe kell venni.

1.2. Egyedi eltérések

1.2.1. Működtetéssel, környezettel kapcsolatos eltérések:

1.2.1.1. A működtetési környezet jellegétől függő biztonsági intézkedések csak akkor alkalmazandók, ha az elektronikus információs rendszert az intézkedéseket szükségessé tevő környezetben használják.

1.2.2. A fizikai infrastruktúrával kapcsolatos eltérések:

1.2.2.1. A szervezeti létesítményekkel kapcsolatos biztonsági intézkedések (zárak, őrök, környezeti paraméterek: hőmérséklet, páratartalom stb.) csak a létesítmény azon részeire alkalmazandók, amelyek közvetlenül nyújtanak védelmet vagy biztonsági támogatást az elektronikus információs rendszernek, vagy kapcsolatosak azzal (ideértve a rendszerelemeket is, mint például e-mail, web szerverek, szerver farmok, adatközpontok, hálózati csomópontok, határvédelmi eszközök és kommunikációs berendezések).

1.2.3. A nyilvános hozzáféréssel kapcsolatos eltérések:

1.2.3.1. A nyilvánosan hozzáférhető információkra vonatkozó biztonsági intézkedéseket körültekintően kell számba venni, és végrehajtani, mivel a vonatkozó védelmi intézkedés katalógus rész egyes biztonsági intézkedései (például azonosítás és hitelesítés, személyi biztonsági intézkedések) nem alkalmazhatók az elektronikus információs rendszerhez engedélyezett nyilvános kapcsolaton keresztül hozzáférő felhasználókra.

1.2.4. Technológiai eltérések:

1.2.4.1. A specifikus technológiára [például vezeték nélküli kommunikáció, kriptográfia, nyilvános kulcsú infrastruktúrán (PKI) alapuló hitelesítési eljárás] vonatkozó biztonsági intézkedések csak akkor alkalmazandók, ha ezeket a technológiákat használják az elektronikus információs rendszerben, vagy előírják ezek használatát.

1.2.4.2. A biztonsági intézkedések az elektronikus információs rendszer csak azon komponenseire vonatkoznak, amelyek az intézkedés által megcélzott biztonsági képességet biztosítják vagy támogatják, és az intézkedés által csökkenteni kívánt lehetséges kockázatok forrásai.

1.2.5. Biztonsági szabályozással kapcsolatos eltérések:

1.2.5.1. A tervezett, vagy már működtetett elektronikus információs rendszerekre alkalmazott biztonsági intézkedések kialakítása során figyelembe kell venni a rendszer célját meghatározó jogszabályi hátteret, funkciót is.

1.2.6. A biztonsági intézkedések bevezetésének fokozatosságával kapcsolatos eltérések:

1.2.6.1. A biztonsági intézkedések fokozatosan vezethetők be. A fokozatosságot a védendő elektronikus információs rendszerek biztonsági kategorizálása alapján lehet felállítani.

1.2.7. A biztonsági célokhoz kapcsolódó eltérések:

1.2.7.1. Azok a biztonsági intézkedések, amelyek kizárólagosan támogatják a bizalmasságot, a sértetlenséget és a rendelkezésre állást, visszasorolhatók (vagy módosíthatók, kivehetők, ha alacsonyabb követelményszinten nincsenek meghatározva) alacsonyabb követelményszintre, ha ez az alacsonyabb szintű besorolás:

1.2.7.1.1. összhangban van a vonatkozó bizalmasságra, sértetlenségre vagy rendelkezésre állásra vonatkozóan az úgynevezett „high water mark” elv alkalmazása előtt megállapított biztonsági követelményszinttel, amely elv az információbiztonság szempontjából azt jelenti, hogy a legmagasabb biztonsági célhoz kell hangolni minden elemet;

1.2.7.1.2. a „high water mark” elv alkalmazásával az eredeti bizalmassági, sértetlenségi és rendelkezésre állási biztonsági célokat meghaladó, magasabb biztonsági intézkedés szint meghatározás történt, de ez a

magasabb biztonsági intézkedési szint nem szükséges a költséghatékony, kockázatarányos biztonsági intézkedések szempontjából;

1.2.7.1.3. az érintett szervezetre végrehajtott kockázatelemzés szerint indokolható;

1.2.7.1.4. nem befolyásolja a biztonsági szempontból fontos információkat az elektronikus információs rendszeren belül.

1.2.7.2. Az elektronikus információs rendszer dokumentáltan elkülönített, informatikai biztonsági szempontból önállóan értékelhető elemei tekintetében a biztonsági intézkedések a szervezet által elfogadott kockázatelemzési és kockázatkezelési eljárásrendben rögzített vizsgálatot követően, külön-külön egyedi eltérésekkel is alkalmazhatóak, ha az elkülönített elemek közötti határvédelemről gondoskodtak. A határvédelem megfelelőségét, valamint az egyedi eltérések okát és mértékét dokumentálni és meghatározott gyakorisággal felülvizsgálni szükséges.

2. HELYETTESÍTŐ BIZTONSÁGI INTÉZKEDÉSEK

2.1. A helyettesítő biztonsági intézkedés olyan eljárás, amelyet az érintett szervezet az adott biztonsági osztályhoz tartozó biztonsági intézkedés helyett alkalmazni kíván, és egyenértékű vagy összemérhető védelmet nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen, és a helyettesített intézkedéssel egyenértékű módon biztosít minden külső vagy belső követelménynek (például törvényeknek vagy szervezeti szintű szabályzóknak) való megfelelést.

2.2. Egy elektronikus információs rendszer esetén az érintett szervezet az alábbi feltételek teljesülése esetén alkalmazhat helyettesítő intézkedést:

2.2.1. ha az elektronikus információs rendszerek biztonságára vonatkozó szabványokban vagy hazai ajánlásokban fellelhető helyettesítő intézkedést választja, vagy ha ezekben nincs megfelelő helyettesítő intézkedés, akkor az érintett szervezet kivételesen alkalmazhat egy, az adott helyzetben megfelelő helyettesítő intézkedést;

2.2.2. a helyettesítő intézkedések kiválasztásánál az érintett szervezetnek törekednie kell arra, hogy a védelmi intézkedés katalógusból válasszon intézkedést; az érintett szervezet által meghatározott helyettesítő intézkedéseket csak végső esetben szabad használni, ha a biztonsági intézkedések katalógusa nem tartalmaz az adott viszonyok között alkalmazható intézkedést;

2.2.3. a vonatkozó szabályozásában be kell mutatnia, hogy a helyettesítő intézkedések hogyan biztosítják az elektronikus információs rendszer egyenértékű biztonsági képességeit, védelmi követelményszintjét, és azt, hogy miért nem használhatók a vonatkozó alapkészlet biztonsági intézkedései;

2.2.4. a 2.2.3. pont szerinti indoklás részletezettségének és szigorúságának az elektronikus információs rendszerre megállapított biztonsági követelményszintnek megfelelőnek kell lennie;

2.2.5. ha felméri, és a kockázatkezelési eljárási rendnek megfelelően elfogadja a helyettesítő intézkedés alkalmazásával kapcsolatos kockázatot;

2.2.6. a helyettesítő biztonsági intézkedések alkalmazását dokumentálja, és az eljárási rendnek megfelelően az érintett személlyel vagy szerepkörrel jóváhagyatja.

3. VÉDELMI INTÉZKEDÉS KATALÓGUS

3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK

3.1.1.1. Informatikai biztonsági szabályzat

3.1.1.1.1. Az érintett szervezet:

3.1.1.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az informatikai biztonsági szabályzatot;

3.1.1.1.1.2. más belső szabályozásában, vagy magában az informatikai biztonsági szabályzatban meghatározza az informatikai biztonsági szabályzat felülvizsgálatának és frissítésének gyakoriságát;

3.1.1.1.1.3. gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.1.1.2. Az informatikai biztonsági szabályzatban meg kell határozni:

3.1.1.1.2.1. a célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően területi) hatályát;

3.1.1.1.2.2. az elektronikus információbiztonsággal kapcsolatos szerepköröket;

3.1.1.1.2.3. a szerepkörhöz rendelt tevékenységet;

3.1.1.1.2.4. a tevékenységhez kapcsolódó felelősséget;

3.1.1.1.2.5. az információbiztonság szervezetrendszerének belső együttműködését.

3.1.1.1.3. Az informatikai biztonsági szabályzat elsősorban a következő elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:

3.1.1.1.3.1. kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz);

3.1.1.1.3.2. biztonsági helyzet-, és eseményértékelés eljárási rendje;

3.1.1.1.3.3. az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzés (ha az érintett szervezet ilyet végez, vagy végezhet);

3.1.1.1.3.4. biztonsággal kapcsolatos tervezés (például: beszerzés, fejlesztés, eljárásrendek kialakítását);

3.1.1.1.3.5. fizikai és környezeti védelem szabályai, jellemzői;

3.1.1.1.3.6. az emberi erőforrásokban rejlő veszélyek megakadályozása (pl.: személyzeti felvételi- és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése, stb.);

3.1.1.1.3.7. az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati, vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében;

3.1.1.1.3.8. az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (ha az érintett szervezetnél ez értelmezhető);

3.1.1.1.3.9. üzlet-, ügy- vagy üzemmenet folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása, stb.);

3.1.1.1.3.10. az elektronikus információs rendszerek karbantartásának rendje;

3.1.1.1.3.11. az adathordozók fizikai és logikai védelmének szabályozása;

3.1.1.1.3.12. az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése;

3.1.1.1.3.13. ha az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása;

3.1.1.1.3.14. az adatok mentésének, archiválásának rendje;

3.1.1.1.3.15. a biztonsági események - ideértve az adatok sérülését is - bekövetkeztekor követendő eljárás, ideértve a helyreállítást;

3.1.1.1.3.16. az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán-, vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények.

3.1.1.1.4. Az informatikai biztonsági szabályzat tartalmazza az érintett szervezet elvárt biztonsági szintjét, valamint az érintett szervezet egyes elektronikus információs rendszereinek elvárt biztonsági osztályát.

3.1.1.2. Az elektronikus információs rendszerek biztonságáért felelős személy

3.1.1.2.1. Az érintett szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg, aki ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 13. §-ában meghatározott feladatokat.

3.1.1.3. Az intézkedési terv és mérföldkövei

3.1.1.3.1. Az érintett szervezet:

3.1.1.3.1.1. intézkedési tervet készít, ebben mérföldköveket határoz meg;

3.1.1.3.1.2. meghatározott időnként felülvizsgálja és karbantartja az intézkedési tervet:

3.1.1.3.1.2.1. a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján;

3.1.1.3.1.2.2. ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, a hiányosság megszüntetése érdekében;

3.1.1.3.1.2.3. ha a meghatározott biztonsági szint alacsonyabb, mint az érintett szervezetre érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, az előírt biztonsági szint elérése érdekében.

3.1.1.3.1.3. folyamatosan aktualizálja a nyilvántartást.

3.1.1.4. Az elektronikus információs rendszerek nyilvántartása

3.1.1.4.1. Az érintett szervezet:

3.1.1.4.1.1. elektronikus információs rendszereiről nyilvántartást vezet;

3.1.1.4.1.2. folyamatosan aktualizálja a nyilvántartást.

3.1.1.4.2. A nyilvántartás minden rendszerre nézve tartalmazza:

3.1.1.4.2.1. annak alapfeladatait;

3.1.1.4.2.2. a rendszerek által biztosítandó szolgáltatásokat;

3.1.1.4.2.3. az érintett rendszerekhez tartozó licenc számot (ha azok az érintett szervezet kezelésében vannak);

3.1.1.4.2.4. a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;

3.1.1.4.2.5. a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

3.1.1.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

3.1.1.5.1. Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó:

3.1.1.5.1.1. emberi, fizikai és logikai erőforrásra;

3.1.1.5.1.2. eljárási és védelmi követelményszintre és folyamatra.

3.1.2. KOCKÁZATELEMZÉS

3.1.2.1. Kockázatelemzési és kockázatkezelési eljárásrend

3.1.2.1.1. Az érintett szervezet:

3.1.2.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatelemzési és kockázatkezelési eljárásrendet, mely a kockázatelemzési és kockázatkezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;

3.1.2.1.1.2. belső szabályozásában, vagy magában a kockázatelemzési és kockázatkezelési eljárásrendről szóló dokumentumban meghatározza a kockázatelemzési és kockázatkezelési eljárásrend felülvizsgálatának és frissítésének gyakoriságát.

3.1.2.1.2. Az eljárásrend kiterjed:

3.1.2.1.2.1. a lehetséges kockázatok felmérésére;

3.1.2.1.2.2. a kockázatok kezelésének felelősségére;

3.1.2.1.2.3. a kockázatok kezelésének elvárt minőségére.

3.1.2.2. Biztonsági osztályba sorolás

3.1.2.2.1. Az érintett szervezet:

3.1.2.2.1.1. jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és a 3.1.1.4. pont szerinti nyilvántartás alapján meghatározza, hogy azok melyik biztonsági osztályba sorolandók;

3.1.2.2.1.2. vezetője jóváhagyja a biztonsági osztályba sorolást;

3.1.2.2.1.3. rögzíti a biztonsági osztályba sorolás eredményét a szervezet informatikai biztonsági szabályzatában.

3.1.2.2.2. Elvárás:

3.1.2.2.2.1. a biztonsági osztályba sorolást az elektronikus információs rendszereket érintő változások után ismételten el kell végezni;

3.1.2.2.2.2. kapcsolódást kell biztosítani a 3.1.1.3. pontban foglalt intézkedési tervhez és mérföldköveihez.

3.1.2.3. Kockázatelemzés

3.1.2.3.1. Az érintett szervezet:

3.1.2.3.1.1. végrehajtja a biztonsági kockázatelemzéseket;

3.1.2.3.1.2. rögzíti a kockázatelemzések eredményét az informatikai biztonsági szabályzatban, kockázatelemzési jelentésben, vagy a kockázatelemzési eljárásrendben előírt dokumentumban;

3.1.2.3.1.3. a kockázatelemzési eljárásrendnek megfelelően felülvizsgálja a kockázatelemzések eredményét;

3.1.2.3.1.4. a kockázatelemzési eljárásrendnek megfelelően, vagy a 3.1.1.1. pont szerinti informatikai biztonsági szabályzata keretében megismerteti a kockázatelemzés eredményét az érintettekkel;

3.1.2.3.1.5. amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését), továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát, ismételt kockázatelemzést hajt végre;

3.1.2.3.1.6. gondoskodik arról, hogy a kockázatelemzési eredmények a jogosulatlanok számára ne legyenek megismerhetők.

3.1.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

3.1.3.0. Jelen címben meghatározott eljárásokat abban az esetben nem kell bevezetni az érintett szervezetnél, ha saját hatókörében informatikai szolgáltatást, vagy eszközöket nem szerez be, és nem végez, vagy végeztet rendszerfejlesztési tevékenységet (ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket). Jelen fejezet alkalmazása szempontjából nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése.

3.1.3.1. Beszerzési eljárásrend

3.1.3.1.1. Az érintett szervezet:

3.1.3.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a beszerzési eljárásrendet, mely az érintett szervezet elektronikus információs rendszerére, az ezekhez kapcsolódó szolgáltatások és információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg (akár az általános beszerzési szabályzat részeként), és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;

3.1.3.1.1.2. a beszerzési eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a beszerzési eljárásrendet.

3.1.3.2. Erőforrás igény felmérés

3.1.3.2.1. Az érintett szervezet:

3.1.3.2.1.1. az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként;

3.1.3.2.1.2. elkülönítetten kezeli az elektronikus információs rendszerek biztonságát beruházás tervezési dokumentumaiban.

3.1.3.3. Beszerzések

3.1.3.3.1. Az érintett szervezet az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza:

3.1.3.3.1.1. a funkcionális biztonsági követelményeket;

3.1.3.3.1.2. a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);

3.1.3.3.1.3. a biztonsággal kapcsolatos dokumentációs követelményeket;

3.1.3.3.1.4. a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;

3.1.3.3.1.5. az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

3.1.3.3.2. A védelem szempontjainak érvényesítése a beszerzés során

Az érintett szervezet védi az elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen.

Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

3.1.3.3.3. A védelmi intézkedések terv-, és megvalósítási dokumentációi

Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas és alacsony szintű biztonsági tervet, - ha azzal a szállító rendelkezik - a forráskódot és futtatókörnyezetet.

3.1.3.3.4. Funkciók - protokollok - szolgáltatások

Az érintett szervezet szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy már a fejlesztési életciklus korai szakaszában meghatározza a használatra tervezett funkciókat, protokollokat és szolgáltatásokat.

3.1.3.4. Az elektronikus információs rendszerre vonatkozó dokumentáció

3.1.3.4.1. Az érintett szervezet:

3.1.3.4.1.1. ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:

3.1.3.4.1.1.1. a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,

3.1.3.4.1.1.2. a biztonsági funkciók hatékony alkalmazását és fenntartását,

3.1.3.4.1.1.3. a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket;

3.1.3.4.1.2. megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza:

3.1.3.4.1.2.1. a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját,

3.1.3.4.1.2.2. a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit,

3.1.3.4.1.2.3. a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;

3.1.3.4.1.3. gondoskodik arról, hogy az információs rendszerre vonatkozó - különösen az adminisztrátori és fejlesztői - dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható;

3.1.3.4.1.4. gondoskodik a dokumentációknak az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

3.1.3.5. Biztonságtervezési elvek

Az érintett szervezet biztonságtervezési elveket dolgoz ki és alkalmaz az elektronikus információs rendszer specifikációjának meghatározása, tervezése, fejlesztése, kivitelezése és módosítása során.

3.1.3.6. Külső elektronikus információs rendszerek szolgáltatásai

3.1.3.6.1. Az érintett szervezet:

3.1.3.6.1.1. szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett szervezet elektronikus információbiztonsági követelményeinek;

3.1.3.6.1.2. meghatározza és dokumentálja az érintett szervezet felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban;

3.1.3.6.1.3. külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

3.1.3.7. Független értékelők

Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmaz a védelmi intézkedések értékelésére.

3.1.3.8. Folyamatos ellenőrzés

3.1.3.8.1. Az érintett szervezet folyamatba épített ellenőrzést vagy ellenőrzési tervet hajt végre, amely tartalmazza:

3.1.3.8.1.1. az ellenőrizendő területeket;

3.1.3.8.1.2. az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát;

3.1.3.8.1.3. az érintett szervezet ellenőrzési stratégiájához illeszkedő folyamatos biztonsági értékeléseket;

3.1.3.8.1.4. a mérőszámok megfelelőségét;

3.1.3.8.1.5. az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését;

3.1.3.8.1.6. az érintett szervezet reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére;

3.1.3.8.1.7. az érintett szervezet döntését arról, hogy milyen gyakorisággal kell az elemzési adatokat általa meghatározott személyi- és szerepkörökkel megismertetni (ideértve azok változásait is).

3.1.3.8.2. Független értékelés

Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmazhat az elektronikus információs rendszer védelmi intézkedéseinek folyamatos ellenőrzésére.

3.1.4. ÜZLETMENET-(ÜGYMENET-)FOLYTONOSSÁG TERVEZÉSE

3.1.4.1. Üzletmenet-folytonosságra vonatkozó eljárásrend

3.1.4.1.1. Az érintett szervezet:

3.1.4.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül az érintett személyi kör részére kihirdeti az elektronikus információs rendszerre vonatkozó eljárásrendet, mely az üzletmenet-folytonosságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.1.4.1.1.2. az üzletmenet-folytonossági tervben, vagy más szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az üzletmenet-folytonosságra vonatkozó eljárásrendet.

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

3.1.4.2.1. Az érintett szervezet:

3.1.4.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet;

3.1.4.2.1.2. összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;

3.1.4.2.1.3. meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;

3.1.4.2.1.4. az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak

megfelelően aktualizálja az üzletmenet-folytonossági tervet;

3.1.4.2.1.5. tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket;

3.1.4.2.1.6. gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;

3.1.4.2.1.7. meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;

3.1.4.2.1.8. rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;

3.1.4.2.1.9. jelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket;

3.1.4.2.1.10. fenntartja a szervezet által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;

3.1.4.2.1.11. kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

3.1.4.2.2. Egyeztetés

Az üzletmenet-folytonossági tervet egyeztetni kell a kapcsolódó, hasonló tervekért felelős szervezeti egységekkel.

3.1.4.2.3. Alapfunkciók újraindítása

Meg kell határozni az alapfunkciók újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követőn.

3.1.4.2.4. Kritikus rendszerelemek meghatározása

Meg kell határozni az elektronikus információs rendszer alapfunkcióit támogató kritikus rendszerelemeket.

3.1.4.2.5. Kapacitástervezés

Meg kell tervezni a folyamatos működéshez szükséges információ-feldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást.

3.1.4.2.6. Összes funkció újraindítása

Meg kell határozni az összes funkció újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követően.

3.1.4.2.7. Alapfeladatok és alapfunkciók folyamatossága

Az alapfeladatok és alapfunkciók folyamatosságát úgy kell megtervezni, hogy azok üzemelési folyamatosságában semmilyen, vagy csak csekély veszteség álljon elő, fenntartható legyen a folyamatosság az elektronikus információs rendszer elsődleges feldolgozó vagy tárolási helyszínén történő teljes helyreállításáig.

3.1.4.3. A folyamatos működésre felkészítő képzés

3.1.4.3.1. Az érintett szervezet az elektronikus információs rendszer folyamatos működésére felkészítő képzést tart a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

3.1.4.3.1.1. szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül;

3.1.4.3.1.2. meghatározott gyakorisággal, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik.

3.1.4.3.2. Szimuláció

A folyamatos működésre felkészítő képzésben szimulált eseményeket kell alkalmazni, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben.

3.1.4.4. Az üzletmenet-folytonossági terv tesztelése

3.1.4.4.1. Az érintett szervezet:

3.1.4.4.1.1. meghatározott gyakorisággal és meghatározott teszteken keresztül vizsgálja az elektronikus információs rendszerre vonatkozó üzletmenet-folytonossági tervet a terv hatékonyságának és az érintett szervezet felkészültségének a felmérése céljából;

3.1.4.4.1.2. értékeli az üzletmenet-folytonossági terv tesztelési eredményeit;

3.1.4.4.1.3. az értékelés alapján szükség esetén javítja a tervet, a javításokkal kapcsolatban az üzletmenet-folytonossági tervre vonatkozó általános eljárási szabályok szerint jár el.

3.1.4.4.2. Koordináció

Az üzletmenet-folytonossági terv tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel egyeztetni kell.

3.1.4.4.3. Tesztelés a tartalék feldolgozási helyszínen

Az üzletmenet folytonossági tervet a tartalék feldolgozási helyszínen is tesztelni kell, hogy az érintett szervezet megismerje az adottságokat és az elérhető erőforrásokat, valamint értékelje a tartalék feldolgozási helyszín képességeit a folyamatos működés támogatására.

3.1.4.5. Biztonsági tárolási helyszín

3.1.4.5.1. Az érintett szervezet kijelöl egy biztonsági tárolási helyszínt, ahol az elektronikus információs rendszer mentéseinek másodlatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja.

3.1.4.5.2. A tartalék feldolgozási helyszín elkülönítése

A biztonsági tárolási helyszínnek el kell különülni az elsődleges tárolás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.

3.1.4.5.3. Üzletmenet-folytonosság elérhetőség

A biztonsági tárolási helyszínhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére - vészhelyzeti eljárásokat kell kidolgozni.

3.1.4.5.4. Üzletmenet folytonosság helyreállítás

A biztonsági tárolási helyszínt úgy kell kialakítani, hogy az elősegítse a helyreállítási tevékenységeket, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

3.1.4.6. Tartalék feldolgozási helyszín

3.1.4.6.1. Az érintett szervezet:

3.1.4.6.1.1. kijelöl egy tartalék feldolgozási helyszínt azért, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésére, elektronikus információs rendszere előre meghatározott műveleteit, előre meghatározott időn belül - összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal - a tartalék helyszínen újra kezdhesse, vagy folytathassa;

3.1.4.6.1.2. biztosítja, hogy a működés újrakezdéséhez, vagy folytatásához szükséges eszközök és feltételek a tartalék feldolgozási helyszínen, vagy meghatározott időn belül rendelkezésre álljanak;

3.1.4.6.1.3. biztosítja, hogy a tartalék feldolgozási helyszín informatikai biztonsági intézkedései egyenértékűek legyenek az elsődleges helyszínen alkalmazottakkal.

3.1.4.6.2. Elkülönítés

Olyan tartalék feldolgozási helyszínt kell kijelölni, amely elkülönül az elsődleges feldolgozás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.

3.1.4.6.3. Elérhetőség

A tartalék feldolgozási helyszínhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére - vészhelyzeti eljárásokat kell kidolgozni.

3.1.4.6.4. Szolgáltatások priorálása a tartalék feldolgozási helyszínen

A tartalék feldolgozási helyszínre vonatkozóan olyan megállapodásokat kell kötni, intézkedéseket kell bevezetni, amelyek a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban álló szolgáltatás-prioritási rendelkezéseket tartalmaznak.

3.1.4.6.5. Előkészület a működés megindítására

Az érintett szervezet úgy készíti fel a tartalék feldolgozási helyszínt, hogy az meghatározott időn belül készen álljon az alapfunkciók működésének támogatására.

3.1.4.7. Infokommunikációs szolgáltatások

3.1.4.7.1. Az érintett szervezet - a Nemzeti Távközlési Gerinchálózatra csatlakozó elektronikus információs rendszerek kivételével - tartalék infokommunikációs szolgáltatásokat létesít, erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

3.1.4.7.2. Szolgáltatás-prioritási rendelkezések

Ha az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

3.1.4.7.3. Közös hibalehetőségek kizárása

Olyan tartalék infokommunikációs szolgáltatásokat kell igénybe venni, melyek csökkentik az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét (pl. alternatív technológiára épülnek).

3.1.4.8. Az elektronikus információs rendszer mentései

3.1.4.8.1. Az érintett szervezet:

3.1.4.8.1.1. meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

3.1.4.8.1.2. meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

3.1.4.8.1.3. meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

3.1.4.8.1.4. megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

3.1.4.8.2. Megbízhatósági és sértetlenségi teszt

Meghatározott gyakorisággal tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének a garantálása érdekében.

3.1.4.8.3. Helyreállítási teszt

Egy kiválasztott mintát kell használni a biztonsági másolat információkból az elektronikus információs rendszer kiválasztott funkcióinak helyreállításánál.

3.1.4.8.4. Kritikus információk elkülönítése

Az érintett szervezet által meghatározott, az elektronikus információs rendszer kritikus szoftvereinek és egyéb biztonsággal kapcsolatos információinak biztonsági másolatait egy elkülönített berendezésen vagy egy minősítéssel rendelkező tűzbiztos tárolóban kell tárolni.

3.1.4.8.5. Alternatív tárolási helyszín

Az elektronikus információs rendszer biztonsági másolat információit a 3.1.4.5. pontban meghatározottak szerinti biztonsági tárolási helyszínen kell tárolni.

3.1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása

3.1.4.9.1. Az érintett szervezet gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

3.1.4.9.2. Tranzakciók helyreállítása

Az érintett szervezet tranzakció alapú elektronikus információs rendszerek esetén tranzakció helyreállítást hajt végre.

3.1.4.9.3. Helyreállítási idő

Az érintett szervezet biztosítja azt a lehetőséget, hogy az elektronikus információs rendszerelemeket előre definiált helyreállítási idő alatt helyre lehessen állítani egy olyan konfigurációellenőrzött és sértetlenség védett információból, ami az elem ismert működési állapotát reprezentálja.

3.1.5. A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

3.1.5.1. Az érintett szervezet:

3.1.5.1.1. eseménykezelési eljárást dolgoz ki a biztonsági eseményekre, amelyek magukban foglalják az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást;

3.1.5.1.2. egyezteti az eseménykezelési eljárásokat az üzletmenet-folytonossági tervéhez tartozó tevékenységekkel;

3.1.5.1.3. az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, a fejlesztési és üzemeltetési eljárásokba, elvárásokba, továbbképzésekbe és tesztelésbe.

3.1.5.2. Automatikus eseménykezelés

Az érintett szervezet automatizált mechanizmusokat alkalmaz az eseménykezelési eljárások támogatására.

3.1.5.3. Információ korreláció

Az érintett szervezet összekapcsolja a biztonsági eseményekre vonatkozó információkat és az egyedi eseményekre való reagálásokat, hogy szervezetszintű rálátást nyerjen a biztonsági eseményekkel kapcsolatos tudatosságra és reagálásokra.

3.1.5.4. A biztonsági események figyelése

3.1.5.4.1. Az érintett szervezet nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit.

3.1.5.5. Automatikus nyomonkövetés, adatgyűjtés és vizsgálat

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események nyomon követését és a biztonsági eseményekre vonatkozó információk gyűjtését és vizsgálatát.

3.1.5.6. A biztonsági események jelentése

3.1.5.6.1. Az érintett szervezet:

3.1.5.6.1.1. mindenkitől, aki az elektronikus információs rendszerrel, vagy azok elhelyezésére szolgáló objektummal kapcsolatban áll megköveteli, hogy jelentsék a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlelnek;

3.1.5.6.1.2. jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek.

3.1.5.6.2. Automatizált jelentés

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események jelentését.

3.1.5.7. Segítségnyújtás a biztonsági események kezeléséhez

3.1.5.7.1. Az érintett szervezet tanácsadást és támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez.

3.1.5.7.2. Automatizált támogatás

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk és a támogatás rendelkezésre állását.

3.1.5.8. Biztonsági eseménykezelési terv

3.1.5.8.1. Az érintett szervezet:

3.1.5.8.1.1. kidolgozza a biztonsági eseménykezelési tervet, amely:

3.1.5.8.1.1.1. az érintett szervezet számára iránymutatást ad a biztonsági esemény kezelési módjaira,

3.1.5.8.1.1.2. ismerteti a biztonsági eseménykezelési lehetőségek struktúráját és szervezetét,

3.1.5.8.1.1.3. átfogó megközelítést nyújt arról, hogy a biztonsági eseménykezelési lehetőségek hogyan illeszkednek az általános szervezetbe,

3.1.5.8.1.1.4. kielégíti az érintett szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit,

3.1.5.8.1.1.5. meghatározza a bejelentésköteles biztonsági eseményeket,

3.1.5.8.1.1.6. meghatározza és folyamatosan pontosítja a biztonsági események kiértékelésének, kategorizálásának (súlyosság, stb.) kritériumrendszerét,

3.1.5.8.1.1.7. támogatást ad a biztonsági eseménykezelési lehetőségek belső mérésére,

3.1.5.8.1.1.8. meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására;

3.1.5.8.1.2. kihirdeti és tudomásul veteti a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő (névvel és/vagy szerepkörrel azonosított) személyeknek és szervezeti egységeknek;

3.1.5.8.1.3. meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet;

3.1.5.8.1.4. frissíti a biztonsági eseménykezelési tervet, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat;

3.1.5.8.1.5. a biztonsági eseménykezelési terv változásait a 3.1.5.8.1.2. pont szerint ismerteti;

3.1.5.8.1.6. gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

3.1.5.9. Képzés a biztonsági események kezelésére

3.1.5.9.1. Az érintett szervezet:

3.1.5.9.1.1. biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban;

3.1.5.9.1.2. a képzést a biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követő, meghatározott időtartamon belül, vagy amikor ezt az elektronikus információs rendszer változásai megkívánják, vagy meghatározott gyakorisággal tartja.

3.1.5.9.2. Szimuláció

Az érintett szervezet a biztonsági esemény kezelési képzésébe szimulált eseményeket foglal, hogy elősegítse a személyzet hatékony reagálását kritikus helyzetekben.

3.1.5.9.3. Automatizált képzési környezet

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy biztonsági esemény kezelési képzéséhez mélyrehatóbb és valószerűbb környezetet biztosítson.

3.1.5.9.4 A biztonsági események kezelésének tesztelése

3.1.5.9.4.1. Az érintett szervezet meghatározott gyakorisággal teszteli az elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességeket előre kidolgozott tesztek felhasználásával, annak érdekében, hogy meghatározza a biztonsági eseménykezelés hatékonyságát, és dokumentálja az eredményeket.

3.1.5.9.4.2. Egyeztetés

Az érintett szervezet egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért (pl. üzletmenet-folytonossági terv és katasztrófaelhárítási terv) felelős szervezeti egységekkel.

3.1.5.9.5 A biztonsági esemény kivizsgálásában részt vevő személynek a megbízása előtt részt kell vennie a biztonságiesemény-kezelő eljárásról szóló, a kormányzati eseménykezelő központ által tartott tájékoztató előadáson.

3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG

3.1.6.1. Személybiztonsági eljárásrend

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.1.6.2. Munkakörök, feladatok biztonsági szempontú besorolása

3.1.6.2.1. Az érintett szervezet:

3.1.6.2.1.1. minden érintett szervezeti munkakört, vagy érintett szervezethez kapcsolódó feladatot biztonsági szempontból besorol;

3.1.6.2.1.2. felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat;

3.1.6.2.1.3. rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

3.1.6.3 A személyek ellenőrzése

3.1.6.3.1. Az érintett szervezet:

3.1.6.3.1.1. az elektronikus információs rendszerhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy a 3.1.6.2.1.1. és 3.1.6.2.1.2. pontok szerinti besorolásnak megfelelő feltételekkel rendelkezik-e;

3.1.6.3.1.2. a 3.1.6.2.1.2. szerinti munkaköröket betöltő vagy feladatokat ellátó személyek tekintetében kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést;

3.1.6.3.1.3. folyamatosan ellenőrzi a 3.1.6.3.1. pont szerinti feltételek fennállását.

3.1.6.4 Eljárás a jogviszony megszűnésekor

3.1.6.4.1. Az érintett szervezet:

3.1.6.4.1.1. belső szabályozásban meghatározott időpontban megszünteti a hozzáférési jogosultságot az elektronikus információs rendszerhez;

3.1.6.4.1.2. megszünteti vagy visszaveszi a személy egyéni hitelesítő eszközeit;

3.1.6.4.1.3. tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről;

3.1.6.4.1.4. visszaveszi az érintett szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;

3.1.6.4.1.5. megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz;

3.1.6.4.1.6. az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;

3.1.6.4.1.7. a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;

3.1.6.4.1.8. a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzi.

3.1.6.5 Az áthelyezések, átirányítások és kirendelések kezelése

3.1.6.5.1. Az érintett szervezet:

3.1.6.5.1.1. szükség esetén elvégzi a 3.1.6.3. pontban foglalt, a személyek ellenőrzésére vonatkozó eljárást;

3.1.6.5.1.2. logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt elektronikus információs rendszerhez;

3.1.6.5.1.3. szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését;

3.1.6.5.1.4. az általa meghatározott módon a jogviszony változásáról értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket.

3.1.6.6. Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

3.1.6.6.1. Az érintett szervezet:

3.1.6.6.1.1. a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az érintett szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;

3.1.6.6.1.2. szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg az érintett szervezet által meghatározott személybiztonsági követelményeknek;

3.1.6.6.1.3. a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket;

3.1.6.6.1.4. előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek;

3.1.6.6.1.5. folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

3.1.6.7. Fegyelmi intézkedések

3.1.6.7.1. Az érintett szervezet:

3.1.6.7.1.1. belső eljárási rendje szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben;

3.1.6.7.1.2. ha az elektronikus információbiztonsági szabályokat nem az érintett szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

3.1.6.8. Belső egyeztetés

Az érintett szervezet tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

3.1.6.9. Viselkedési szabályok az interneten

3.1.6.9.1. Az érintett szervezet:

3.1.6.9.1.1. tiltja és számon kéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;

3.1.6.9.1.2. tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységet (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.);

3.1.6.9.1.3. tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a szervezettől idegen tevékenységet.

3.1.7. TUDATOSSÁG ÉS KÉPZÉS

3.1.7.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel

3.1.7.1.1. Az érintett szervezet:

3.1.7.1.1.1. az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek folyamatos oktatásának, képzésének elősegítése;

3.1.7.1.1.2. az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása;

3.1.7.1.1.3. a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel.

3.1.7.2. Képzési eljárásrend

3.1.7.2.1. Az érintett szervezet:

3.1.7.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a képzési eljárásrendet, mely a képzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.1.7.2.1.2. a képzési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a képzési eljárásrendet.

3.1.7.3. Biztonság tudatosság képzés

3.1.7.3.1. Az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára:

3.1.7.3.1.1. az új felhasználók kezdeti képzésének részeként;

3.1.7.3.1.2. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;

3.1.7.3.1.3. az érintett szervezet által meghatározott gyakorisággal.

3.1.7.4. Belső fenyegetés

A biztonságtudatossági képzés az érintett személyeket készítse fel a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket.

3.1.7.5. Szerepkör, vagy feladat alapú biztonsági képzés

3.1.7.5.1. Az érintett szervezet szerepkör, vagy feladat alapú biztonsági képzést nyújt az egyes szerepkörök szerinti, azért felelős személyeknek:

3.1.7.5.1.1. az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;

3.1.7.5.1.2. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;

3.1.7.5.1.3. az érintett szervezet által meghatározott rendszerességgel.

3.1.7.6. A biztonsági képzésre vonatkozó dokumentációk

3.1.7.6.1. Az érintett szervezet:

3.1.7.6.1.1. dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket;

3.1.7.6.1.2. a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi.

3.2. FIZIKAI VÉDELMI INTÉZKEDÉSEK

3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

3.2.1.1. Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre, valamint arra, hogy e fejezet rendelkezései az adott létesítmény bárki által szabadon látogatható, vagy igénybe vehető területeire nem vonatkoznak.

3.2.1.2. Fizikai védelmi eljárásrend

3.2.1.2.1. Az érintett szervezet:

3.2.1.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerek szempontjából érintett létesítményekre vagy helyiségekre érvényes fizikai védelmi eljárásrendet, amely az érintett szervezet elektronikus információbiztonsági vagy egyéb szabályzatának részét képező fizikai védelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.2.1.2.1.2. a fizikai védelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a fizikai védelmi eljárásrendet.

3.2.1.3. Fizikai belépési engedélyek

3.2.1.3.1. Az érintett szervezet:

3.2.1.3.1.1. összeállítja, jóváhagyja, és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;

3.2.1.3.1.2. belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépéshez a belépni szándékozó részére;

3.2.1.3.1.3. rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;

3.2.1.3.1.4. eltávolítja a belépésre jogosult személyek listájáról azokat, akik a belépésre már nem jogosultak;

3.2.1.3.1.5. intézkedik a 3.2.1.3.1.2. pont szerinti dokumentum visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.

3.2.1.4. A fizikai belépés ellenőrzése

3.2.1.4.1. Az érintett szervezet:

3.2.1.4.1.1. kizárólag az érintett szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;

3.2.1.4.1.2. naplózza a fizikai belépéseket;

3.2.1.4.1.3. ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;

3.2.1.4.1.4. kíséri a létesítménybe ad-hoc belépésre jogosultakat, és figyelemmel követi a tevékenységüket;

3.2.1.4.1.5. megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközt;

3.2.1.4.1.6. nyilvántartást vezet a fizikai belépést ellenőrző eszközről;

3.2.1.4.1.7. meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;

3.2.1.4.1.8. az egyéni belépési engedélyeket a belépési pontokon ellenőrzi;

3.2.1.4.1.9. a kijelölt pontokon való átjutást felügyeli a szervezet által meghatározott fizikai belépést ellenőrző rendszerrel vagy eszközzel;

3.2.1.4.1.10. felhívja a szervezet tagjainak figyelmét a rendellenességek jelentésére.

3.2.1.4.2. Hozzáférés az információs rendszerhez

Az érintett szervezet a létesítménybe történő fizikai belépés ellenőrzésén túl külön engedélyhez köti a fizikai belépést az elektronikus információs rendszereknek helyt adó helyiségekbe is.

3.2.1.5. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

Az érintett szervezet az általa meghatározott biztonsági védelemmel ellenőrzi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

3.2.1.6. A kimeneti eszközök hozzáférés ellenőrzése

Az érintett szervezet ellenőrzi az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá.

3.2.1.7. A fizikai hozzáférések felügyelete

3.2.1.7.1. Az érintett szervezet:

3.2.1.7.1.1. ellenőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és reagáljon arra;

3.2.1.7.1.2. rendszeresen átvizsgálja a fizikai hozzáférésekről készült naplókat;

3.2.1.7.1.3. azonnal átvizsgálja a fizikai hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak;

3.2.1.7.1.4. összehangolja a biztonsági események kezelését, valamint a napló átvizsgálások eredményét.

3.2.1.7.2. Behatolás riasztás, felügyeleti berendezések

Az érintett szervezet felügyeli a fizikai behatolás riasztásokat és a felügyeleti berendezéseket.

3.2.1.7.3. Az elektronikus információs rendszerekhez való hozzáférés felügyelete

Az érintett szervezet a létesítménybe való fizikai belépések ellenőrzésén felül külön felügyeli az elektronikus információs rendszer egy vagy több elemét tartalmazó helyiségekbe történő fizikai belépéseket.

3.2.1.8. A látogatók ellenőrzése

3.2.1.8.1. Az érintett szervezet:

3.2.1.8.1.1. meghatározott ideig megőrzi az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat;

3.2.1.8.1.2. azonnal átvizsgálja a látogatói belépésekről készített információkat és felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak.

3.2.1.8.2. Automatizált látogatói információkezelés

Az érintett szervezet automatizált mechanizmusokat alkalmaz a látogatói belépésekről készített információk és felvételek kezeléséhez, átvizsgálásához.

3.2.1.9. Áramellátó berendezések és kábelezés

Az érintett szervezet védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben.

3.2.1.9.1. Tartalék áramellátás

Az érintett szervezet az elsődleges áramforrás kiesése esetére, a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.

3.2.1.9.2. Hosszútávú tartalék áramellátás a minimálisan elvárt működési képességhez

Az érintett szervezet az elsődleges áramforrás kiesése esetén biztosítja a hosszútávú tartalék áramellátást az elektronikus információs rendszer minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására.

3.2.1.10. Vészkikapcsolás

3.2.1.10.1. Az érintett szervezet:

3.2.1.10.1.1. lehetőséget biztosít az elektronikus információs rendszer vagy egyedi rendszerelemek áramellátásának kikapcsolására vészhelyzetben;

3.2.1.10.1.2. gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről;

3.2.1.10.1.3. megakadályozza a jogosulatlan vészkikapcsolást.

3.2.1.11. Vészvilágítás

Az érintett szervezet egy automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

3.2.1.12. Tűzvédelem

3.2.1.12.1. Az érintett szervezet az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.

3.2.1.12.2. Automatikus tűzelfojtás

Az érintett szervezet a személyzet által folyamatosan nem felügyelt elektronikus információs rendszerek számára automatikus tűzelfojtási képességet biztosít.

3.2.1.12.3. Észlelő berendezések, rendszerek

Az érintett szervezet az elektronikus információs rendszer védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld az érintett szervezet által kijelölt tűzvédelmi felelősnek.

3.2.1.12.4. Tűzelfojtó berendezések, rendszerek

Az érintett szervezet az elektronikus információs rendszer védelmére olyan tűzelfojtó berendezést vagy rendszert alkalmaz, amelynek aktiválásáról automatikusan jelzést kap az érintett szervezet által kijelölt tűzvédelmi felelős.

3.2.1.13. Hőmérséklet és páratartalom ellenőrzés

3.2.1.13.1. Az érintett szervezet:

3.2.1.13.1.1. az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) az erőforrások biztonságos működéséhez szükséges szinten tartja a hőmérsékletet és páratartalmat;

3.2.1.13.1.2. az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) figyeli a hőmérséklet és páratartalom szintjét.

3.2.1.14. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

3.2.1.14.1. Az érintett szervezet:

3.2.1.14.1.1. védi az elektronikus információs rendszert a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek;

3.2.1.14.1.2. az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. adatközpont, szerver szoba, központi gépterem) során biztosítja, hogy az a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével is.

3.2.1.14.2. Automatizált védelem

Az érintett szervezet automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer közelében megjelenő folyadékszivárgás észlelésére és az érintett szervezet által kijelölt személyek riasztására.

3.2.1.15. Be- és kiszállítás

Az érintett szervezet engedélyezi, vagy tiltja, továbbá figyeli és ellenőrzi a létesítménybe bevitt, onnan kivitt információs rendszerelemeket, és nyilvántartást vezet ezekről.

3.2.1.16. Az elektronikus információs rendszer elemeinek elhelyezése

Az érintett szervezet úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

3.2.1.17. Ellenőrzés

Az érintett szervezet ellenőrzi a karbantartó személyzet által a létesítménybe hozott karbantartási eszközöket, a nem megfelelő vagy jogosulatlan módosítások megakadályozása érdekében.

3.2.1.18. Szállítási felügyelet

3.2.1.18.1. Az érintett szervezet védi az információt tartalmazó karbantartási eszközt a jogosulatlan elszállítással szemben azzal, hogy:

3.2.1.18.1.1. ellenőrzi, az eszköz nem tartalmaz-e információt;

3.2.1.18.1.2. ha az eszköz tartalmaz információt, azt törli vagy megsemmisíti;

3.2.1.18.1.3. az eszközt a létesítményen belül őrzi;

3.2.1.18.1.4. az ezért felelős személyekkel engedélyezteti az eszköz elszállítását a létesítményből.

3.2.1.19. Karbantartók

3.2.1.19.1. Az érintett szervezet:

3.2.1.19.1.1. kialakít egy folyamatot a karbantartók munkavégzési engedélyének kezelésére, és nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;

3.2.1.19.1.2. megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;

3.2.1.19.1.3. felhatalmazást ad a szervezethez tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

3.2.1.19.2. Karbantartás fokozott biztonsági intézkedésekkel

3.2.1.19.2.1. Az érintett szervezet:

3.2.1.19.2.1.1. a megfelelő biztonsági engedéllyel nem rendelkező karbantartó személyek alkalmazása során:

3.2.1.19.2.1.1.1. az ilyen karbantartó személyeket megfelelő hozzáférési jogosultságú, műszakilag képzett belső személyekkel felügyelete alatt tartja az elektronikus információs rendszeren végzett karbantartási és diagnosztikai tevékenységek során,

3.2.1.19.2.1.1.2. a karbantartási és diagnosztikai tevékenységek megkezdése előtt az elektronikus információs rendszer minden fellelhető információtároló elemét törli, és a nem törölhető adathordozót eltávolítja, vagy fizikailag leválasztja a rendszertől;

3.2.1.19.2.1.2. alternatív biztonsági védelmet alakít ki, ha egy elektronikus információs rendszerelemet nem lehet törölni, eltávolítani vagy a rendszertől leválasztani.

3.2.1.19.3. Időben történő javítás

Az érintett szervezet karbantartási támogatást szerez be a meghatározott elektronikus információs rendszerelemekhez.

3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK

3.3.1. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

3.3.1.1. Az érintett szervezet:

3.3.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat;

3.3.1.1.2. felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát;

3.3.1.1.3. meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket, kijelöli az ezeket betöltő személyeket;

3.3.1.1.4. integrálja az elektronikus információbiztonsági engedélyezési folyamatokat a szervezeti szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.

3.3.1.2. Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó:

3.3.1.2.1. emberi, fizikai és logikai erőforrásra;

3.3.1.2.2. eljárási és védelmi szintre és folyamatra.

3.3.1.3. Az elektronikus információs rendszer kapcsolódásai

3.3.1.3.1. Az érintett szervezet:

3.3.1.3.1.1. szabályozza, és belső engedélyhez kötheti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez;

3.3.1.3.1.2. dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

3.3.1.3.2. Belső rendszer kapcsolatok

az érintett szervezet belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását;

3.3.1.3.3. Külső kapcsolódásokra vonatkozó korlátozások

Az érintett szervezet a külső elektronikus információs rendszerekhez való kapcsolódásokhoz az informatikai biztonsági szabályzatában szabályrendszert állít fel, és alkalmaz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

3.3.1.4. Személybiztonság

3.3.1.4.1. Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az érintett szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki az érintett szervezet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az érintett szervezet tagja, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.3.2. TERVEZÉS

3.3.2.1. Biztonságtervezési szabályzat

3.3.2.1.1. Az érintett szervezet:

3.3.2.1.1.1. megfogalmazza, az érintett szervezetre érvényes követelmények szerint dokumentálja, és a munka- és feladatkörük miatt érintettek számára kihirdeti a biztonságtervezési szabályzatot, amely tartalmazza a biztonságtervezési eljárás folyamatait, valamint biztosítja annak ellenőrzését;

3.3.2.1.1.2. a biztonságtervezési szabályzatban, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságtervezési szabályzatot.

3.3.2.2. Rendszerbiztonsági terv

3.3.2.2.1. Az érintett szervezet, ha az elektronikus információs rendszer tervezése a hatókörébe tartozik, az elektronikus információs rendszerhez rendszerbiztonsági tervet készít, amely:

3.3.2.2.1.1. összhangban áll szervezeti felépítésével vagy szervezeti szintű architektúrájával;

3.3.2.2.1.2. meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;

3.3.2.2.1.3. meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;

3.3.2.2.1.4. meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;

3.3.2.2.1.5. a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit;

3.3.2.2.1.6. meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;

3.3.2.2.1.7. gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és

szerepkörökben dolgozók megismerjék (ideértve annak változásait is);

3.3.2.2.1.8. belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét;

3.3.2.2.1.9. frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;

3.3.2.2.1.10. elvégzi a szükséges belső egyeztetéseket;

3.3.2.2.1.11. gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

3.3.2.3. Cselekvési terv

3.3.2.3.1. Az érintett szervezet:

3.3.2.3.1.1. cselekvési tervet készít, ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg;

3.3.2.3.1.2. a cselekvési tervben dokumentálja a megállapított hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeit;

3.3.2.3.1.3. frissíti a meglévő cselekvési tervet az érintett szervezet által meghatározott gyakorisággal a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján.

3.3.2.4. Személyi biztonság

3.3.2.4.1. Az érintett szervezet:

3.3.2.4.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységet;

3.3.2.4.1.2. az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja;

3.3.2.4.1.3. meghatározott gyakorisággal felülvizsgálja, és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységet a viselkedési szabályok betartását;

3.3.2.4.1.4. gondoskodik arról, hogy a 3.3.2.4.1.3. pont szerinti változás esetén a hozzáféréssel rendelkezők tekintetében a

3.3.2.4.1.2. pont szerinti eljárás megtörténjen;

3.3.2.4.1.5. meghatározza az érintett szervezeten kívüli irányban megvalósuló követelményeket.

3.3.2.5. Információbiztonsági architektúra leírás

3.3.2.5.1. Az érintett szervezet (ha a hatókörébe tartozik, és ha más dokumentumban nem kerül meghatározásra, vagy azokból nem következik):

3.3.2.5.1.1. elkészíti az elektronikus információs rendszer információbiztonsági architektúra leírását;

3.3.2.5.1.2. az általános architektúrájában bekövetkezett változtatásokra reagálva felülvizsgálja, és frissíti az információbiztonsági architektúra leírást;

3.3.2.5.1.3. biztosítja, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön a rendszerbiztonsági tervben és a beszerzésekben.

3.3.2.5.2. Az információbiztonsági architektúra leírás:

3.3.2.5.2.1. összegzi az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló filozófiát, követelményeket és megközelítést;

3.3.2.5.2.2. megfogalmazza, hogy az információbiztonsági architektúra miként illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt;

3.3.2.5.2.3. leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket.

3.3.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

3.3.3.1. Jelen címben meghatározott eljárásokat abban az esetben nem kell bevezetni az érintett szervezetnél, ha saját hatókörében informatikai szolgáltatást vagy eszközöket nem szerez be, és nem végez, vagy végeztet rendszerfejlesztési tevékenységet (ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket). Jelen fejezet alkalmazása szempontjából nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése.

3.3.3.2. A rendszer fejlesztési életciklusa

3.3.3.2.1. Az érintett szervezet:

3.3.3.2.1.1. elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket;

3.3.3.2.1.2. a fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket;

3.3.3.2.1.3. meghatározza, és a szervezetre érvényes szabályok szerint kijelöli az információbiztonsági szerepköröket betöltő, felelős személyeket.

3.3.3.2.2. A rendszer életciklus szakaszai a következők:

3.3.3.2.2.1. követelmény meghatározás;

3.3.3.2.2.2. fejlesztés vagy beszerzés;

3.3.3.2.2.3. megvalósítás vagy értékelés;

3.3.3.2.2.4. üzemeltetés és fenntartás;

3.3.3.2.2.5. kivonás (archiválás, megsemmisítés).

3.3.3.3. Funkciók, portok, protokollok, szolgáltatások

Az érintett szervezet megköveteli, hogy a szolgáltató meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

3.3.3.4. Fejlesztői változáskövetés

3.3.3.4.1. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

3.3.3.4.1.1. vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során;

3.3.3.4.1.2. dokumentálja, kezelje, és ellenőrizze a változtatásokat, biztosítsa ezek sértetlenségét;

3.3.3.4.1.3. csak a jóváhagyott változtatásokat hajtsa végre az elektronikus információs rendszeren, rendszerelemen vagy rendszerszolgáltatáson;

3.3.3.4.1.4. dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait;

3.3.3.4.1.5. kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit az érintett szervezet által meghatározott személyeknek.

3.3.3.5. Fejlesztői biztonsági tesztelés

3.3.3.5.1. Az érintett szervezet megköveteli, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője:

3.3.3.5.1.1. készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat;

3.3.3.5.1.2. hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, vagy regressziós tesztelést, és ezt értékelje ki az érintett szervezet által meghatározott lefedettség és mélység mellett;

3.3.3.5.1.3. dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat, és ismertesse a biztonsági tesztelés és értékelés eredményeit;

3.3.3.5.1.4. javítsa ki a biztonsági tesztelés és értékelés során feltárt hiányosságokat.

3.3.3.6. Fejlesztési folyamat, szabványok és eszközök

3.3.3.6.1. Az érintett szervezet:

3.3.3.6.1.1. megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentált fejlesztési folyamatot kövessen;

3.3.3.6.1.2. előírja, hogy az általa meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat.

3.3.3.6.2. A dokumentált fejlesztési folyamat:

3.3.3.6.2.1. kiemelten kezeli a biztonsági követelményeket;

3.3.3.6.2.2. meghatározza a fejlesztés során alkalmazott szabványokat és eszközöket;

3.3.3.6.2.3. dokumentálja a fejlesztés során alkalmazott speciális eszköz opciókat és konfigurációkat;

3.3.3.6.2.4. nyilvántartja a változtatásokat, és biztosítja ezek engedély nélküli megváltoztatás elleni védelmét.

3.3.3.7. Fejlesztői oktatás

Az érintett szervezet oktatási kötelezettséget ír elő az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára, hogy az érintett szervezet által kijelölt személyek - elsősorban adminisztrátorok - és biztonsági felelősök a megvalósított biztonsági funkciók, intézkedések és mechanizmusok helyes használatát és működését megismerhessék és elsajátíthassák.

3.3.3.8. Fejlesztői biztonsági architektúra és tervezés

3.3.3.8.1. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan specifikációt és biztonsági architektúrát hozzon létre, amely:

3.3.3.8.1.1. illeszkedik a szervezet biztonsági architektúrájához és támogatja azt;

3.3.3.8.1.2. leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között;

3.3.3.8.1.3. bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében.

3.3.4. BIZTONSÁGI ELEMZÉS

3.3.4.1. Biztonságelemzési eljárásrend

3.3.4.1.1. Az érintett szervezet:

3.3.4.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.4.1.1.2. a biztonságértékelési eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a biztonságértékelési eljárásrendet.

3.3.4.2. Biztonsági értékelések

3.3.4.2.1. Az érintett szervezet:

3.3.4.2.1.1. biztonságértékelési tervet készít;

3.3.4.2.1.2. meghatározott gyakorisággal értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését;

3.3.4.2.1.3. elkészíti a biztonságértékelés eredményét összefoglaló jelentést;

3.3.4.2.1.4. gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.

3.3.4.2.2. A biztonsági értékelés tartalmazza:

3.3.4.2.2.1. az értékelendő (adminisztratív, fizikai és logikai) védelmi intézkedéseket;

3.3.4.2.2.2. a biztonsági ellenőrzések eredményességét meghatározó eljárásrendeket;

3.3.4.2.2.3. az értékelési környezetet, az értékelő csoportot, az értékelés célját, az értékelést végzők feladatát.

3.3.4.3. Speciális értékelés

Az érintett szervezet a védelmi intézkedések értékelése keretében bejelentés mellett, vagy bejelentés nélkül sérülékenységvizsgálatot, rosszhiszemű felhasználó tesztet, belső fenyegetettség értékelést, a biztonságkritikus egyedi fejlesztésű szoftverelemek forráskód elemzését, az érintett szervezet által meghatározott egyéb biztonsági értékeléseket végeztet.

3.3.4.4. A biztonsági teljesítmény mérése

Az érintett szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

3.3.5. TESZTELÉS, KÉPZÉS ÉS FELÜGYELET

3.3.5.1. Az érintett szervezet:

3.3.5.1.1. ha ez hatókörébe tartozik, megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint kihirdeti az elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárásokat, amelyek támogatják a tesztelési, képzési és felügyeleti tevékenységek:

3.3.5.1.1.1. fejlesztését és fenntartását;

3.3.5.1.1.2. folyamatos időbeni végrehajtását;

3.3.5.1.1.3. felülvizsgálja a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.

3.3.5.2. A biztonsági teljesítmény mérése

Az érintett szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

3.3.5.3. Sérülékenység teszt

3.3.5.3.1. Az érintett szervezet:

3.3.5.3.1.1. az elektronikus információs rendszerei és alkalmazásai tekintetében sérülékenység tesztet végez, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik;

3.3.5.3.1.2. meghatározott gyakorisággal, vagy véletlenszerűen, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban, megismétli a sérülékenység tesztet;

3.3.5.3.1.3. a sérülékenység tesztet sérülékenységvizsgálati eszközök és technikák alkalmazásával, vagy külső szervezet bevonásával azon elektronikus információs rendszerek tekintetében végzi el, amelyek az érintett szervezet felügyelete, irányítása alatt állnak;

3.3.5.3.1.4. kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról;

3.3.5.3.1.5. végrehajtja az ellenőrzési listákat és tesztelési eljárásokat;

3.3.5.3.1.6. felméri a sérülékenység lehetséges hatásait;

3.3.5.3.1.7. elemzi a sérülékenység teszt eredményét;

3.3.5.3.1.8. megosztja a sérülékenység teszt eredményét a szervezet által meghatározott személyekkel és szerepkörökkel.

3.3.5.3.2. Frissítési képesség

Az érintett szervezet olyan sérülékenységi teszteszközt alkalmaz, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel.

3.3.5.3.3. Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően

Az érintett szervezet az elektronikus információs rendszerre vizsgált sérülékenység körét aktualizálja az új tesztet megelőzően, vagy a sérülékenység feltárását követően azonnal.

3.3.5.3.4. Privilegizált hozzáférés

Az elektronikus információs rendszer különleges jogosultsághoz kötött - úgynevezett privilegizált - hozzáférést biztosít az érintett szervezet által kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.

3.3.5.3.5. Felfedhető információk

Az érintett szervezet meghatározza, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javításokat hajt végre.

3.3.6. KONFIGURÁCIÓKEZELÉS

3.3.6.1. Konfigurációkezelési eljárásrend

3.3.6.1.1. Az érintett szervezet:

3.3.6.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a konfigurációkezelési eljárásrendet, mely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.6.1.1.2. a fizikai védelmi eljárásrendben, vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a konfigurációkezelési eljárásrendet.

3.3.6.2. Alapkonfiguráció

3.3.6.2.1. Az érintett szervezet az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.

3.3.6.2.2. Áttekintések és frissítések

Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni.

3.3.6.2.3. Korábbi konfigurációk megőrzése

Változatlan állapotban meg kell őrizni az elektronikus információs rendszer alapkonfigurációját és annak további verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés.

3.3.6.2.4. Magas kockázatú területek konfigurálása

3.3.6.2.4.1. Biztonsági szempontokból meghatározott módon konfigurált elektronikus információs rendszerelemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják.

3.3.6.2.4.2. Megfelelő biztonsági eljárásokat kell alkalmazni a 3.3.6.2.4.1. pont szerinti eszköz belső használatba vonásakor.

3.3.6.2.5. Automatikus támogatás

Automatikus mechanizmusokat kell alkalmazni az elektronikus információs rendszer naprakész, teljes, pontos, és állandóan rendelkezésre álló alapkonfigurációjának a karbantartására.

3.3.6.3. A konfigurációváltozások felügyelete (változáskezelés)

3.3.6.3.1. Az érintett szervezet:

3.3.6.3.1.1. meghatározza a változáskezelési felügyelet alá eső változástípusokat;

3.3.6.3.1.2. meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek, stb.);

3.3.6.3.1.3. megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja vagy elutasítja azokat;

3.3.6.3.1.4. dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;

3.3.6.3.1.5. megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;

3.3.6.3.1.6. visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását;

3.3.6.3.1.7. auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

3.3.6.3.2. Előzetes tesztelés és megerősítés

A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

3.3.6.3.3. Automatikus támogatás

3.3.6.3.3.1. Automatikus mechanizmusokat kell alkalmazni:

3.3.6.3.3.1.1. az elektronikus információs rendszerben javasolt változtatások dokumentálására;

3.3.6.3.3.1.2. a jóváhagyásra jogosultak értesítésére;

3.3.6.3.3.1.3. a késedelmes jóváhagyások kiemelésére;

3.3.6.3.3.1.4. a még nem jóváhagyott változások végrehajtásának a megakadályozására;

3.3.6.3.3.1.5. az elektronikus információs rendszerben végrehajtott változások teljes dokumentálására;

3.3.6.3.3.1.6. a jóváhagyásra jogosultak értesítésére a jóváhagyott változtatások végrehajtásáról.

3.3.6.4. Biztonsági hatásvizsgálat

3.3.6.4.1. Az érintett szervezet megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását, még a változtatások megvalósítása előtt.

3.3.6.4.2. Elkülönített tesztkörnyezet

Az érintett szervezet a változtatásokat éles rendszerben történő megvalósításuk előtt egy elkülönített tesztkörnyezetben vizsgálja, hibákat, sebezhetőségeket, kompatibilitási problémákat és szándékos károkozásra utaló jeleket keresve.

3.3.6.5. A változtatásokra vonatkozó hozzáférés korlátozások

3.3.6.5.1. Az érintett szervezet az elektronikus információs rendszerre vonatkozóan szabályozásában meghatározza a változtatásokhoz való hozzáférési jogosultságot, dokumentálja a hozzáférési jogosultságokat, jóváhagyja azokat, fizikai és logikai hozzáférés korlátozásokat alkalmaz az elektronikus információs rendszer változtatásaival kapcsolatban.

3.3.6.5.2. Automatikus támogatás

Az érintett szervezet az elektronikus információs rendszerben automatikus mechanizmusokat alkalmaz a hozzáférési korlátozások érdekében, az ezzel kapcsolatos tevékenység naplózására.

3.3.6.5.3. Felülvizsgálat

Az érintett szervezet rendszeresen felülvizsgálja az elektronikus információs rendszer változtatásait annak megállapítására, hogy történt-e jogosulatlan változtatás.

3.3.6.5.4. Aláírt elemek

A szervezet által meghatározott szoftver- és az úgynevezett firmware (vezérlőeszköz) elemek esetében meg kell akadályozni az elemek telepítését, ha azok nincsenek digitálisan aláírva ismert és jóváhagyott tanúsítvány alkalmazásával.

3.3.6.6. Konfigurációs beállítások

3.3.6.6.1. Az érintett szervezet:

3.3.6.6.1.1. meghatározza a működési követelményeknek még megfelelő, de biztonsági szempontból a lehető leginkább korlátozott módon - a „szükséges minimum” elv alapján - az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja;

3.3.6.6.1.2. elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;

3.3.6.6.1.3. a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést;

3.3.6.6.1.4. figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, az érintett szervezet belső szabályzataival és eljárásaival összhangban.

3.3.6.6.2. Automatikus támogatás

Az érintett szervezet az elektronikus információs rendszerre vonatkozóan automatikus mechanizmusokat alkalmaz a konfigurációs beállítások központi kezelésére, alkalmazására és ellenőrzésére.

3.3.6.6.3. Reagálás jogosulatlan változásokra

Az érintett szervezet meghatározott intézkedéseket vezet be a meghatározott konfigurációs beállítások jogosulatlan változtatásai esetén.

3.3.6.7. Legszűkebb funkcionalitás

3.3.6.7.1. Az érintett szervezet:

3.3.6.7.1.1. az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges

szolgáltatásokat nyújtsa;

3.3.6.7.1.2. meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

3.3.6.7.2. Rendszeres felülvizsgálat

3.3.6.7.2.1. Az érintett szervezet meghatározott gyakorisággal átvizsgálja az elektronikus információs rendszert, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.

3.3.6.7.2.2. Az érintett szervezetnek a szoftver használatra meghatározott szabályzatainak vagy a szoftver használatára vonatkozó feltételeinek és kikötéseinek megfelelően az elektronikus információs rendszer megakadályozza a tiltott programok futtatását.

3.3.6.7.3. Nem futtatható szoftverek

Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját, és megtiltja ezek futtatását.

3.3.6.7.4. Futtatható szoftverek

Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben jogosultan futtatható (engedélyezett, úgynevezett fehérlistás) szoftverek listáját, és engedélyezi ezek futtatását, az ettől eltérő szoftver futtatását egyedi engedélyhez köti.

3.3.6.8. Elektronikus információs rendszerelem leltár

3.3.6.8.1. Az érintett szervezet:

3.3.6.8.1.1. leltárt készít az elektronikus információs rendszer elemeiről;

3.3.6.8.1.2. meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt;

3.3.6.8.1.3. gondoskodik arról, hogy a leltár:

3.3.6.8.1.3.1. pontosan tükrözze az elektronikus információs rendszer aktuális állapotát;

3.3.6.8.1.3.2. az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza;

3.3.6.8.1.3.3. legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

3.3.6.8.2. Frissítés

Az érintett szervezet az elektronikus információs rendszerelem leltárt frissíti az egyes rendszerelemek telepítésének, eltávolításának, frissítésének időpontjában.

3.3.6.8.3. Jogosulatlan elemek automatikus észlelése

3.3.6.8.3.1. Automatizált mechanizmusok biztosítják, hogy a szervezet által meghatározott gyakorisággal a jogosulatlan hardver-, szoftver- és firmware elemek észlelése megtörténjen.

3.3.6.8.3.2. A jogosulatlan elemek észlelése esetén le kell tiltani az ilyen elemek általi hálózati hozzáférést, el kell őket különíteni, és értesíteni kell az illetékes személyeket.

3.3.6.8.4. Duplikálás elleni védelem

Az érintett szervezet ellenőrzi, hogy az elektronikus információs rendszer hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.

3.3.6.8.5. Automatikus támogatás

Az érintett szervezet automatikus mechanizmusokat alkalmaz az elektronikus információs rendszerelem leltár naprakész, teljes, pontos, és állandóan rendelkezésre álló kezelésének támogatására.

3.3.6.8.6. Naplózás

Az elektronikus információs rendszerelem leltárhoz csatolni kell az egyes elemek adminisztrálásáért felelős személyek nevét, pozícióját vagy szerepkörét.

3.3.6.9. Konfigurációkezelési terv

3.3.6.9.1. Az érintett szervezet:

3.3.6.9.1.1. kialakít, dokumentál és végrehajt egy, az elektronikus információs rendszerre vonatkozó konfigurációkezelési tervet, mely figyelembe veszi a szerepköröket, felelősségeket, konfigurációkezelési folyamatokat és eljárásokat;

3.3.6.9.1.2. bevezet egy folyamatot a konfigurációelemek azonosítására a rendszer-fejlesztési életciklus

folyamán és a konfigurációelemek konfigurációjának kezelésére;

3.3.6.9.1.3. meghatározza az elektronikus információs rendszer konfigurációelemeit, és a konfigurációelemeket a konfigurációkezelés alá helyezi;

3.3.6.9.1.4. védi a konfigurációkezelési tervet a jogosulatlan felfedéssel és módosítással szemben.

3.3.6.10. A szoftverhasználat korlátozásai

3.3.6.10.1. Az érintett szervezet:

3.3.6.10.1.1. kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak;

3.3.6.10.1.2. a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;

3.3.6.10.1.3. ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

3.3.6.11. A felhasználó által telepített szoftverek

3.3.6.11.1. Az érintett szervezet:

3.3.6.11.1.1. megfogalmazza az elektronikus információs rendszer vonatkozásában, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti azokat a szabályokat, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségét;

3.3.6.11.1.2. érvényesíti a szoftvertelepítésre vonatkozó szabályokat az érintett szervezet által meghatározott módszerek szerint;

3.3.6.11.1.3. meghatározott gyakorisággal ellenőrzi a szabályok betartását.

3.3.7. KARBANTARTÁS

3.3.7.1. Rendszer karbantartási eljárásrend

3.3.7.1.1. Az érintett szervezet:

3.3.7.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.7.1.1.2. a fizikai védelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a rendszer karbantartási eljárásrendet.

3.3.7.2. Rendszeres karbantartás

3.3.7.2.1. Az érintett szervezet:

3.3.7.2.1.1. a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a szervezeti követelményeknek megfelelően;

3.3.7.2.1.2. jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;

3.3.7.2.1.3. az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a szervezeti létesítményből;

3.3.7.2.1.4. az elszállítás előtt minden adatot és információt - mentést követően - töröl a berendezésről;

3.3.7.2.1.5. ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;

3.3.7.2.1.6. csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.

3.3.7.2.2. Automatikus támogatás

3.3.7.2.2.1. Az érintett szervezet:

3.3.7.2.2.1.1. automatizált mechanizmusokat alkalmaz a karbantartások és javítások ütemezésére, lefolytatására és dokumentálására;

3.3.7.2.2.1.2. naprakész, pontos és teljes nyilvántartást készít minden igényelt, ütemezett, folyamatban lévő és befejezett karbantartási és javítási akcióról.

3.3.7.3. Karbantartási eszközök

3.3.7.3.1. Az érintett szervezet az elektronikus információs rendszer vonatkozásában jóváhagyja, nyilvántartja, és ellenőrzi az elektronikus információs rendszer karbantartási eszközeit.

3.3.7.3.2. Adathordozó ellenőrzés

Az érintett szervezet ellenőrzi a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

3.3.7.4. Távoli karbantartás

3.3.7.4.1. Az érintett szervezet:

3.3.7.4.1.1. jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket;

3.3.7.4.1.2. akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az informatikai biztonsági szabályzattal, és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében;

3.3.7.4.1.3. hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál;

3.3.7.4.1.4. nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről;

3.3.7.4.1.5. lezárja a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.

3.3.7.4.2. Dokumentálás

Az érintett szervezet az elektronikus információs rendszer rendszerbiztonsági tervében dokumentálja a távoli karbantartási és diagnosztikai kapcsolatok létrehozására és használatára vonatkozó szabályokat és eljárásokat.

3.3.7.4.3. Összehasonlítható biztonság

3.3.7.4.3.1. Az érintett szervezet megköveteli, hogy a távoli karbantartási és diagnosztikai javítások olyan elektronikus információs rendszerből legyenek végrehajtva, amelyben a biztonsági képességek azonos szintűek a szervizelt rendszer biztonsági képességekkel.

3.3.7.4.3.2. Ha a 3.3.7.4.3.1. pont szerinti eljárás nem biztosított, a szervizelendő elemet el kell távolítani az elektronikus információs rendszerből, és a távoli karbantartási és diagnosztikai szervizelést megelőzően minden információt törölni kell az érintett rendszerelemről.

3.3.7.4.3.3. Ha a 3.3.7.4.3.1. vagy a 3.3.7.4.3.2. pont szerinti eljárást nem lehet lefolytatni, a szervizelés végrehajtását követően át kell vizsgálni az elemet a lehetséges kártékony szoftverek miatt, mielőtt visszakapcsoljak az elektronikus információs rendszerhez.

3.3.8. ADATHORDOZÓK VÉDELME

3.3.8.1. Adathordozók védelmére vonatkozó eljárásrend

3.3.8.1.1. Az érintett szervezet:

3.3.8.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az adathordozók védelmére vonatkozó eljárásrendet, mely az adathordozókra vonatkozó védelmi szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.8.1.1.2. az adathordozók védelmére vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az adathordozók védelmére vonatkozó eljárásrendet.

3.3.8.2. Hozzáférés az adathordozókhoz

Az érintett szervezet az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát meghatározza.

3.3.8.3. Adathordozók címkézése

Az érintett szervezet megjelöli az elektronikus információs rendszer adathordozóit, jelezve az

információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket, ha ezek rendelkezésre állnak.

3.3.8.4. Adathordozók tárolása

3.3.8.4.1. Az érintett szervezet:

3.3.8.4.1.1. fizikailag ellenőrzi és biztonságosan tárolja az adathordozókat, az arra engedélyezett vagy kijelölt helyen;

3.3.8.4.1.2. védi az elektronikus információs rendszer adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.

3.3.8.5. Adathordozók szállítása

3.3.8.5.1. Az érintett szervezet:

3.3.8.5.1.1. meghatározott biztonsági óvintézkedésekkel védi és ellenőrzi az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán;

3.3.8.5.1.2. biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás folyamán;

3.3.8.5.1.3. dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket;

3.3.8.5.1.4. korlátozza az adathordozók szállításával kapcsolatos tevékenységeket az arra jogosult személyekre.

3.3.8.5.2. Kriptográfiai védelem

Kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás folyamán.

3.3.8.6. Adathordozók törlése

3.3.8.6.1. Az érintett szervezet:

3.3.8.6.1.1. a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt;

3.3.8.6.1.2. a törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza.

3.3.8.6.2. Ellenőrzés

Az érintett szervezet felülvizsgálja, jóváhagyja, nyomon követi, dokumentálja, és ellenőrzi az adathordozók törlésével és megsemmisítésével kapcsolatos tevékenységeket.

3.3.8.6.3. Tesztelés

A törlésre alkalmazott eszközöket és eljárásokat meghatározott gyakorisággal tesztelni kell.

3.3.8.6.4. Törlés megsemmisítés nélkül

Nem romboló törlési technikák alkalmazhatók a meghatározott hordozható tárolóeszközökre, mielőtt ilyen eszközöket az elektronikus információs rendszerhez csatolnak.

3.3.8.7. Adathordozók használata

3.3.8.7.1. Az érintett szervezet engedélyezi, korlátozza, vagy tiltja egyes, vagy bármely adathordozó típusok használatát a meghatározott elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával.

3.3.8.7.2. Ismeretlen tulajdonos

Az érintett szervezet megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS

3.3.9.1. Azonosítási és hitelesítési eljárásrend

3.3.9.1.1. Az érintett szervezet:

3.3.9.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az azonosítási és hitelesítésre vonatkozó eljárásrendet, mely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.9.1.1.2. az azonosítási és hitelesítésre vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti az azonosítási és hitelesítésre vonatkozó eljárásrendet.

3.3.9.2. Azonosítás és hitelesítés

3.3.9.2.1. Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a szervezet felhasználóit, a felhasználók által végzett tevékenységet.

3.3.9.2.2. Hálózati hozzáférés privilegizált fiókokhoz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.9.2.3. Hálózati hozzáférés nem privilegizált fiókokhoz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.9.2.4. Helyi hozzáférés privilegizált fiókokhoz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

3.3.9.2.5. Visszajátszás-védelem

Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.9.2.6. Távoli hozzáférés - külön eszköz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy, az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek.

3.3.9.2.7. Helyi hozzáférés nem privilegizált fiókokhoz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

3.3.9.2.8. Visszajátszás ellen védett hálózati hozzáférés nem privilegizált fiókokhoz

Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.9.3. Eszközök azonosítása és hitelesítése

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköz típusokat mielőtt helyi vagy távoli hálózati kapcsolatot létesítene velük.

3.3.9.4. Azonosító kezelés

3.3.9.4.1. Az érintett szervezet:

3.3.9.4.1.1. az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a szervezet által meghatározott személyek vagy szerepkörök jogosultságához köti;

3.3.9.4.1.2. hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz vagy eszközhöz;

3.3.9.4.1.3. meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását;

3.3.9.4.1.4. meghatározott időtartamú inaktivitás esetén letiltja az azonosítót.

3.3.9.5. A hitelesítésre szolgáló eszközök kezelése

3.3.9.5.1. Az érintett szervezet:

3.3.9.5.1.1. ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;

3.3.9.5.1.2. meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;

3.3.9.5.1.3. biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;

3.3.9.5.1.4. dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;

3.3.9.5.1.5. megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;

3.3.9.5.1.6. meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét,

valamint ismételt felhasználhatóságának feltételeit;

3.3.9.5.1.7. a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;

3.3.9.5.1.8. megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;

3.3.9.5.1.9. megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;

3.3.9.5.1.10. lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

3.3.9.5.2. Jelszó (tudás) alapú hitelesítés

3.3.9.5.2.1. Az érintett szervezet:

3.3.9.5.2.1.1. a jelszóra a következő elvárásokat érvényesíti: kis- és nagybetűk megkülönböztetése; a karakterek számának meghatározása; a kisbetűk, nagybetűk, számok és speciális karakterek, és minimális jelszóhosszúság;

3.3.9.5.2.1.2. meghatározott szám karakterváltozást kényszerít ki új jelszó létrehozásakor;

3.3.9.5.2.1.3. a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást), és nem továbbítja;

3.3.9.5.2.1.4. a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy, hogy meghatározott számú új jelszóig megtiltja a jelszavak ismételt felhasználását, és a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez.

3.3.9.5.3. Birtoklás alapú hitelesítés

3.3.9.5.3.1. Az érintett szervezet:

3.3.9.5.3.1.1. az elektronikus információs rendszer hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel az érintett szervezet által meghatározott minőségi követelményeknek, vagy

3.3.9.5.3.1.2. az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén:

3.3.9.5.3.1.2.1. ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;

3.3.9.5.3.1.2.2. kikényszeríti a megfelelő magánkulcshoz való jogosult hozzáférést;

3.3.9.5.3.1.2.3. összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal;

3.3.9.5.3.1.2.4. megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

3.3.9.5.4. Tulajdonság alapú hitelesítés

Az érintett szervezet a felhasználó egyedi azonosítást lehetővé tevő tulajdonságai alapján végzi el az azonosítást.

3.3.9.5.5. Személyes vagy megbízható harmadik fél általi regisztráció

Az érintett szervezet meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet folytat le az érintett szervezet által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

3.3.9.6. A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

3.3.9.7. Hitelesítés kriptográfiai modul esetén

Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

3.3.9.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

3.3.9.8.1. Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett szervezeten kívüli felhasználókat és tevékenységüket.

3.3.9.8.2. Hitelesítésszolgáltatók tanúsítványának elfogadása

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus

aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE

3.3.10.1. Hozzáférés ellenőrzési eljárásrend

3.3.10.1.1. Az érintett szervezet:

3.3.10.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.10.1.1.2. a hozzáférés védelmére vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja és frissíti a hozzáférések védelmére vonatkozó eljárásrendet.

3.3.10.2. Felhasználói fiókok kezelése

3.3.10.2.1. Az érintett szervezet:

3.3.10.2.1.1. meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;

3.3.10.2.1.2. kijelöli a felhasználói fiókok fiókkezelőit;

3.3.10.2.1.3. kialakítja a csoport- és szerepkör tagsági feltételeket;

3.3.10.2.1.4. meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;

3.3.10.2.1.5. létrehozza, engedélyezi, módosítja, letiltja, és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;

3.3.10.2.1.6. ellenőrzi a felhasználói fiókok használatát;

3.3.10.2.1.7. értesíti a fiókkezelőket, ha:

3.3.10.2.1.7.1. a felhasználói fiókokra már nincsen szükség,

3.3.10.2.1.7.2. a felhasználók kiléptek vagy áthelyezésre kerültek,

3.3.10.2.1.7.3. az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;

3.3.10.2.1.8. feljogosít az elektronikus információs rendszerhez való hozzáférésre:

3.3.10.2.1.8.1. az érvényes hozzáférési engedély,

3.3.10.2.1.8.2. a tervezett rendszerhasználat,

3.3.10.2.1.8.3. az alapfeladatok és funkcióik alapján;

3.3.10.2.1.9. meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot;

3.3.10.2.1.10. kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök vagy adatok újra kibocsátására (ha ilyet alkalmaznak), a csoport tagjainak változása esetére.

3.3.10.2.2. Automatikus kezelés

Az elektronikus információs rendszer automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer fiókjainak kezeléséhez.

3.3.10.2.3. Ideiglenes fiókok eltávolítása

Meghatározott időtartam letelte után az elektronikus információs rendszer automatikusan eltávolítja vagy letiltja az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat vagy egyes kijelölt felhasználói fiók típusokat.

3.3.10.2.4. Inaktív fiókok letiltása

Az elektronikus információs rendszer automatikusan letiltja az inaktív fiókokat meghatározott időtartam letelte után.

3.3.10.2.5. Automatikus naplózás

Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával,

engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket.

3.3.10.2.6. Kiléptetés

Meghatározott időtartamú várható inaktivitás vagy egyéb előre meghatározott esetekben ki kell léptetni a felhasználót.

3.3.10.2.7. Szokatlan használat

Figyelni kell az elektronikus információs rendszer fiókjait az érintett szervezet által meghatározott szokatlan használat szempontjából, és meghatározott személyeknek vagy szerepköröknek jelenteni kell azt.

3.3.10.2.8. Letiltás

Azonnal le kell tiltani a kockázatot jelentő felhasználók fiókjait.

3.3.10.3. Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

3.3.10.4. Információáramlás ellenőrzés érvényesítése

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzéséhez az érintett szervezet által meghatározott információáramlás ellenőrzési szabályoknak megfelelően.

3.3.10.5. A felelősségek szétválasztása

3.3.10.5.1. Az érintett szervezet:

3.3.10.5.1.1. szétválasztja az egyéni felelősségeket;

3.3.10.5.1.2. dokumentálja az egyéni felelősségek szétválasztását;

3.3.10.5.1.3. meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

3.3.10.6. Legkisebb jogosultság elve

3.3.10.6.1. Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

3.3.10.6.2. Jogosult hozzáférés a biztonsági funkciókhoz

Az érintett szervezet hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

3.3.10.6.3. Nem privilegizált hozzáférés a biztonsági funkciókhoz

Az érintett szervezet kötelezővé teszi, hogy a szervezet meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják.

3.3.10.6.4. Privilegizált fiókok

Az érintett szervezet az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

3.3.10.6.5. Privilegizált funkciók használatának naplózása

Az elektronikus információs rendszer naplózza a privilegizált funkciók végrehajtását.

3.3.10.6.6. Privilegizált funkciók tiltása nem privilegizált felhasználóknak

Az elektronikus információs rendszer megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését, vagy megváltoztatását.

3.3.10.6.7. Hálózati hozzáférés a privilegizált parancsokhoz

A meghatározott privilegizált parancsok hálózaton keresztüli elérését csak meghatározott üzemeltetési szükséghelyzetben lehet engedélyezni, és az ilyen hozzáférések indoklását dokumentálni kell a rendszerbiztonsági tervben. Privilegizált parancsok csak meghatározott munkaállomásokról, terminálokról, szegmensekről és IP címekről adhatóak ki, mely munkaállomások/terminálok helyiségei

fizikai hozzáférés szempontjából normáltól eltérő szintű besorolást kapnak.

3.3.10.7. Sikertelen bejelentkezési kísérletek

3.3.10.7.1. Az elektronikus információs rendszer:

3.3.10.7.1.1. az érintett szervezet által meghatározott esetszám korlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire;

3.3.10.7.1.2. ha a sikertelen bejelentkezési kísérletekre felállított esetszám korlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.

3.3.10.8. A rendszerhasználat jelzése

3.3.10.8.1. Az érintett szervezet az elektronikus információs rendszer felhasználásával:

3.3.10.8.1.1. az érintett szervezet által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelzi, hogy:

3.3.10.8.1.1.1. a felhasználó az érintett szervezet elektronikus információs rendszerét használja;

3.3.10.8.1.1.2. a rendszer használatot figyelhetik, rögzíthetik, naplózhatják;

3.3.10.8.1.1.3. a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;

3.3.10.8.1.1.4. a rendszer használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti.

3.3.10.8.2. Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez.

3.3.10.8.3. Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén:

3.3.10.8.3.1. kijelzi a rendszer használat feltételeit, mielőtt további hozzáférést biztosít;

3.3.10.8.3.2. ha felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak;

3.3.10.8.3.3. leírást biztosít a rendszer engedélyezett felhasználásáról.

3.3.10.9. Egyidejű munkaszakasz kezelés

Az érintett szervezet az elektronikus információs rendszerben meghatározott számra korlátozza az egyidejű munkaszakaszok számát, a meghatározott fiókok vagy fiók típusok számára külön-külön.

3.3.10.10. A munkaszakasz zárolása

3.3.10.10.1. Az érintett szervezet:

3.3.10.10.1.1. meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;

3.3.10.10.1.2. megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

3.3.10.10.2. Képernyőtakarás

A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - kell eltakarni.

3.3.10.11. A munkaszakasz lezárása

Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

3.3.10.12. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

3.3.10.12.1. Az érintett szervezet:

3.3.10.12.1.1. kijelöli azokat a felhasználói tevékenységeket, amelyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül is végre lehet hajtani;

3.3.10.12.1.2. dokumentálja és indokolja a rendszerbiztonsági tervben, vagy más szabályzatban az azonosítás vagy hitelesítés nélkül is végrehajtható felhasználói tevékenységeket.

3.3.10.13. Távoli hozzáférés

3.3.10.13.1. Az érintett szervezet:

3.3.10.13.1.1. kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat;

3.3.10.13.1.2. engedélyezési eljárást folytat le az elektronikus információs rendszerhez történő távoli hozzáférés feltételeként.

3.3.10.13.2. Ellenőrzés

Az elektronikus információs rendszer figyeli és ellenőrzi a távoli hozzáféréseket.

3.3.10.13.3. Titkosítás

Kriptográfiai mechanizmusokat kell alkalmazni a távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére.

3.3.10.13.4. Hozzáférés ellenőrzési pontok

Minden távoli hozzáférést felügyelt hozzáférés ellenőrzési ponton keresztül kell irányítani az elektronikus információs rendszerben.

3.3.10.13.5. Privilegizált parancsok elérése

3.3.10.13.5.1. Az érintett szervezet:

3.3.10.13.5.1.1. privilegizált parancsok végrehajtásához és biztonságkritikus információk eléréséhez távoli hozzáférést csak meghatározott és elfogadott igény esetén engedélyez;

3.3.10.13.5.1.2. dokumentálja és indokolja a 3.3.10.13.5.1.1. pont szerinti hozzáféréseket a rendszerbiztonsági tervben.

3.3.10.14. Vezeték nélküli hozzáférés

3.3.10.14.1. Az érintett szervezet:

3.3.10.14.1.1. belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;

3.3.10.14.1.2. engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

3.3.10.14.2. Hitelesítés és titkosítás

Az érintett szervezet az elektronikus információs rendszerben titkosítással, és a felhasználók, vagy eszközök hitelesítésével védi a vezeték nélküli hozzáférést.

3.3.10.14.3. Felhasználó konfigurálás tiltása

Az érintett szervezet azonosítja a felhasználókat, és csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül teszi lehetővé számukra a vezeték nélküli hálózat független konfigurálását.

3.3.10.14.4. Antennák

Az érintett szervezet olyan karakterisztikájú és teljesítményszintű antennákat és árnyékolási megoldásokat üzemeltet, vagy egyéb technikákat alkalmaz, amelyekkel csökkenti az érintett szervezet fizikai védelmi határain kívül a jelek észlelésének a valószínűségét.

3.3.10.15. Mobil eszközök hozzáférés ellenőrzése

3.3.10.15.1. Az érintett szervezet:

3.3.10.15.1.1. belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre;

3.3.10.15.1.2. engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

3.3.10.15.2. Titkosítás

Az érintett szervezet teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

3.3.10.16. Külső elektronikus információs rendszerek használata

3.3.10.16.1. Az érintett szervezet:

3.3.10.16.1.1. meghatározza, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;

3.3.10.16.1.2. meghatározza, hogy külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani az érintett szervezet által ellenőrzött

információkat.

3.3.10.16.2. Korlátozott használat

3.3.10.16.2.1. Az érintett szervezet csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az által ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:

3.3.10.16.2.1.1. előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját szabályzóinak megfelelő módon; vagy

3.3.10.16.2.1.2. jóváhagyott kapcsolat van az elektronikus információs rendszerek között, vagy megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

3.3.10.16.3. Hordozható adattároló eszközök

Az érintett szervezet korlátozza vagy megtiltja az ellenőrzött hordozható tárolóeszközök használatát külső elektronikus információs rendszerben is jogosultsággal rendelkező személyek számára.

3.3.10.17. Információmegosztás

3.3.10.17.1. Az érintett szervezet:

3.3.10.17.1.1. elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet;

3.3.10.17.1.2. automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információmegosztási vagy együttműködési döntések meghozatalában.

3.3.10.18. Nyilvánosan elérhető tartalom

3.3.10.18.1. Az érintett szervezet:

3.3.10.18.1.1. kijelöli azokat a személyeket, akik jogosultak a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett szervezettel kapcsolatos bármely információ közzétételére;

3.3.10.18.1.2. a 3.3.10.18.1.1. pont szerinti kijelölt személyeket képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;

3.3.10.18.1.3. közzététel előtt átvizsgálja a javasolt tartalmat;

3.3.10.18.1.4. meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében, és eltávolítja azokat.

3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

3.3.11.1. Ezeket a rendelkezéseket egy adott elektronikus információs rendszer tekintetében abban az esetben kell alkalmazni, ha az adott elektronikus információs rendszert az érintett szervezet üzemelteti. Üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell érvényesíteni a 3.3.11. pontban és alpontjaiban foglaltakat, és azokat a szolgáltatónak kell biztosítania.

3.3.11.2. Rendszer- és információsértetlenségre vonatkozó eljárásrend

3.3.11.2.1. Az érintett szervezet:

3.3.11.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer- és információsértetlenségre vonatkozó eljárásrendet, mely a szervezet informatikai biztonsági szabályzatának részét képező, rendszer- és információsértetlenségre vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.11.2.1.2. a rendszer- és információsértetlenségre vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a rendszer- és információsértetlenségre vonatkozó eljárásrendet.

3.3.11.3. Hibajavítás

3.3.11.3.1. Az érintett szervezet:

3.3.11.3.1.1. azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit;

3.3.11.3.1.2. telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket az érintett szervezet feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából;

3.3.11.3.1.3. a biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíti vagy telepítteti;

3.3.11.3.1.4. beépíti a hibajavítást a konfigurációkezelési folyamatba.

3.3.11.3.2. Automatizált hibajavítási állapot

Az érintett szervezet automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer elemei hibajavítási állapotának meghatározására.

3.3.11.3.3. Központi kezelés

Az érintett szervezet központilag kezeli a hibajavítás folyamatát.

3.3.11.4. Kártékony kódok elleni védelem

3.3.11.4.1. Az érintett szervezet:

3.3.11.4.1.1. az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat;

3.3.11.4.1.2. frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

3.3.11.4.1.3. konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:

3.3.11.4.1.3.1. rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtsa végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, a hálózati belépési vagy kilépési pontokon, a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,

3.3.11.4.1.3.2. a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt, és riassza a rendszeradminisztrátort és az érintett szervezet által meghatározott további személy(eke)t;

3.3.11.4.1.4. ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

3.3.11.4.2. Központi kezelés

Az elektronikus információs rendszer központilag kezeli a kártékony kódok elleni védelmi mechanizmusokat.

3.3.11.4.3. Automatikus frissítés

Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

3.3.11.5. Az elektronikus információs rendszer felügyelete

3.3.11.5.1. Az érintett szervezet:

3.3.11.5.1.1. felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;

3.3.11.5.1.2. azonosítja az elektronikus információs rendszer jogosulatlan használatát;

3.3.11.5.1.3. felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére, és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;

3.3.11.5.1.4. védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;

3.3.11.5.1.5. erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;

3.3.11.5.1.6. meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

3.3.11.5.2. Automatizálás

Automatizált eszközöket kell alkalmazni az események közel valós idejű vizsgálatának támogatására.

3.3.11.5.3. Felügyelet

Az elektronikus információs rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy

jogosulatlan tevékenységekre vagy körülményre tekintettel.

3.3.11.5.4. Riasztás

Az elektronikus információs rendszer riassza az érintett szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

3.3.11.6. Biztonsági riasztások és tájékoztatások

3.3.11.6.1. Az érintett szervezet:

3.3.11.6.1.1. folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;

3.3.11.6.1.2. folyamatosan figyelemmel kíséri a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;

3.3.11.6.1.3. szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;

3.3.11.6.1.4. a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;

3.3.11.6.1.5. kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel;

3.3.11.6.1.6. megfelelő ellenintézkedéseket és válaszlépéseket tesz.

3.3.11.6.2. Automatikus riasztások

Mechanizmusokat kell kialakítani a biztonsági riasztások és figyelmeztetések szervezeten belüli elérhetőségének biztosítására.

3.3.11.7. A biztonsági funkcionalitás ellenőrzése

3.3.11.7.1. Az elektronikus információs rendszer:

3.3.11.7.1.1. ellenőrzi a beállított biztonsági funkciókat az ellenőrzésre jogosult felhasználó utasítására, vagy időszakosan;

3.3.11.7.1.2. értesítést küld az érintett szervezet által meghatározott személyeknek vagy szerepköröknek, ha az ellenőrzés hibát tár fel;

3.3.11.7.1.3. rendellenesség észlelése esetén leállítja a rendszert, az érintett szerv által alkalmazott döntése szerint újraindítja a rendszert, vagy egyéb ellenintézkedést valósít meg.

3.3.11.8. Szoftver- és információsértetlenség

3.3.11.8.1. Az érintett szervezet sértetlenség ellenőrző eszközt alkalmaz a szoftverek és információk jogosulatlan módosításának észlelésére.

3.3.11.8.2. Sértetlenség ellenőrzés

Az elektronikus információs rendszer sértetlenség ellenőrzést hajt végre a meghatározott szoftverekre és információkra, a rendszer újraindításakor, vagy biztonsági esemény bekövetkezését követően, vagy meghatározott gyakorisággal.

3.3.11.8.3. Észlelés és reagálás

Az érintett szervezet beépíti az elektronikus információs rendszer jogosulatlan változtatásainak észlelését a biztonsági eseményekre reagáló eljárásaiba.

3.3.11.8.4. Automatikus értesítés

Az érintett szervezet automatizált eszközöket alkalmaz a meghatározott személyek vagy szerepkörök értesítésére, ha a sértetlenség ellenőrzés rendellenességet tár fel.

3.3.11.8.5. Automatikus reagálás

Az elektronikus információs rendszer automatikusan leállítja vagy újraindítja a rendszert, vagy egyéb intézkedést valósít meg, ha a sértetlenség ellenőrzés rendellenességet tár fel.

3.3.11.8.6. Végrehajtható kód

Az elektronikus információs rendszer megtiltja az olyan bináris vagy gépi kód használatát, amely nem ellenőrzött forrásból származik, vagy amelynek forráskódjával nem rendelkezik.

3.3.11.9. Kéretlen üzenetek elleni védelem

3.3.11.9.1. Az érintett szervezet:

3.3.11.9.1.1. kéretlen üzenetek - úgynevezett levélszemét - elleni védelmet valósít meg az elektronikus információs rendszer belépési és kilépési pontjain, a levélszemét észlelése és kiszűrése érdekében;

3.3.11.9.1.2. új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabályzattal és eljárásrenddel.

3.3.11.9.2. Központi kezelés

Az érintett szervezet központi beállításokkal irányítja a levélszemét elleni védelmet.

3.3.11.9.3. Frissítés

Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival.

3.3.11.10. Bemeneti információ ellenőrzés

Az elektronikus információs rendszer ellenőrzi a meghatározott információ belépési pontok érvényességét.

3.3.11.11. Hibakezelés

3.3.11.11.1. Az elektronikus információs rendszer:

3.3.11.11.1.1. hibajelzéseket generál a hibajavításhoz szükséges információkat biztosítva, ugyanakkor nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak;

3.3.11.11.1.2. a hibajelzéseket kizárólag a meghatározott személyek vagy szerepkörök számára teszi elérhetővé.

3.3.11.12. A kimeneti információ kezelése és megőrzése

Az érintett szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

3.3.11.13. Memóriavédelem

Az elektronikus információs rendszerben biztonsági beállításokat kell alkalmazni azért, hogy védje a memóriát a jogosulatlan kódok végrehajtásától.

3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

3.3.12.1. Naplózási eljárásrend

3.3.12.1.1. Az érintett szervezet:

3.3.12.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül a szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a naplózási eljárásrendet, mely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.12.1.1.2. a naplózásra és elszámoltathatóságra vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a naplózási eljárásrendet.

3.3.12.2. Naplózható események

3.3.12.2.1. Az érintett szervezet:

3.3.12.2.1.1. meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét;

3.3.12.2.1.2. egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;

3.3.12.2.1.3. megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

3.3.12.2.2. Felülvizsgálat

Az érintett szervezet meghatározott gyakorisággal felülvizsgálja, és aktualizálja a naplózandó eseményeket.

3.3.12.3. Naplóbejegyzések tartalma

3.3.12.3.1. Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

3.3.12.3.2. Kiegészítő információk

Az elektronikus információs rendszer a naplóbejegyzésekben további, az érintett szervezet által meghatározott kiegészítő, részletesebb információkat is rögzít.

3.3.12.3.3. Központi kezelés

Az elektronikus információs rendszer biztosítja a meghatározott rendszerelemek által generált naplóbejegyzések tartalmának központi kezelését és konfigurálását.

3.3.12.4. Napló tárkapacitás

Az érintett szervezet a naplózásra elegendő méretű tárkapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével.

3.3.12.5. Naplózási hiba kezelése

3.3.12.5.1. Az elektronikus információs rendszer:

3.3.12.5.1.1. naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek;

3.3.12.5.1.2. elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását.

3.3.12.5.2. Naplózási tárhely ellenőrzés

Az elektronikus információs rendszer figyelmezteti a meghatározott személyeket, szerepköröket és helyszíneket, ha a lefoglalt naplózási tárhely eléri a beállított maximális naplózási tárhely előre meghatározott részét.

3.3.12.5.3. Valósidejű riasztás

Az elektronikus információs rendszer riasztást küld, ha a meghatározott, valós idejű riasztást igénylő hibaesemények listája szerint valamely esemény megtörténik.

3.3.12.6. Naplóvizsgálat és jelentéskészítés

3.3.12.6.1. Az érintett szervezet:

3.3.12.6.1.1. rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából;

3.3.12.6.1.2. jelenti ezeket a meghatározott személyeknek vagy szerepköröknek.

3.3.12.6.2. Folyamatba illesztés

Az érintett szervezet automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a veszélyes vagy tiltott tevékenységekre és történésekre reagál.

3.3.12.6.3. Összegzés

Az érintett szervezet megvizsgálja és összefüggésbe hozza a különböző adattárakban található naplóbejegyzéseket, a teljes érintett szervezetre kiterjedő helyzetfelmérés érdekében.

3.3.12.6.4. Felügyeleti képességek integrálása

Az érintett szervezet egyesíti a naplóbejegyzések vizsgálatát a sebezhetőség ellenőrzési információkkal, a teljesítmény adatokkal, az elektronikus információs rendszer felügyeletéből származó információkkal, vagy egyéb forrásokból begyűjtött adatokkal vagy információkkal.

3.3.12.6.5. Összekapcsolás a fizikai hozzáférési információkkal

Az érintett szervezet összefüggésbe hozza a naplóbejegyzésekből származó információkat a fizikai hozzáférés felügyeletéből nyert információkkal.

3.3.12.7. Naplócsökkentés és jelentéskészítés

3.3.12.7.1. Az elektronikus információs rendszer:

3.3.12.7.1.1. lehetőséget biztosít naplócsökkentésre és jelentés készítésére, amely támogatja az igény esetén végzendő naplóáttekintési, naplóvizsgálati és jelentéskészítési követelményeket és a biztonsági eseményeket követő tényfeltáró vizsgálatait;

3.3.12.7.1.2. nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.

3.3.12.7.2. Automatikus feldolgozás

Az elektronikus információs rendszer biztosítja, hogy a fontos naplóbejegyzéseket automatikusan fel lehessen dolgozni.

3.3.12.8. Időbélyegek

3.3.12.8.1. Az elektronikus információs rendszer:

3.3.12.8.1.1. belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához;

3.3.12.8.1.2. időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz - úgynevezett GMT - rendelhető módon, megfelelve az érintett szervezet

által meghatározott időmérési pontosságnak.

3.3.12.8.2. Szinkronizálás

Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

3.3.12.9. A naplóinformációk védelme

3.3.12.9.1. Az elektronikus információs rendszer megvédi a naplóinformációt és a napló kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

3.3.12.9.2. Hozzáférés korlátozása

A naplófunkciók kezelésére csak az érintett szervezet által meghatározott, privilegizált felhasználók jogosultak.

3.3.12.9.3. Fizikailag elkülönített mentés

Az elektronikus információs rendszer a naplóbejegyzéseket meghatározott gyakorisággal elmenti, egy a keletkezési helyétől fizikailag elkülönülő rendszerre vagy rendszerelemre.

3.3.12.9.4. Kriptográfiai védelem

Kriptográfiai mechanizmusokat kell alkalmazni a naplóinformáció és a napló kezelő eszköz sértetlenségének védelmére.

3.3.12.10. Letagadhatatlanság

Az elektronikus információs rendszer védelmet biztosít az ellen, hogy egy adott személy az általa használt alkalmazás tekintetében letagadhassa, hogy elvégzett-e egy, a letagadhatatlanság követelménye alá sorolt tevékenységet.

3.3.12.11. A naplóbejegyzések megőrzése

Az érintett szervezet a naplóbejegyzéseket meghatározott - a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

3.3.12.12. Naplógenerálás

3.3.12.12.1. Az elektronikus információs rendszer:

3.3.12.12.1.1. biztosítja a naplóbejegyzés generálási lehetőségét a 3.3.12.2. pontban meghatározott naplózható eseményekre;

3.3.12.12.1.2. lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;

3.3.12.12.1.3. naplóbejegyzéseket állít elő a 3.3.12.2. pont szerinti eseményekre a 3.3.12.3. pontban meghatározott tartalommal.

3.3.12.12.2. Rendszerszintű időalap napló

Az elektronikus információs rendszer a naplóbejegyzéseiből rendszerszintű (logikai vagy fizikai) felülvizsgálati naplót állít össze, amely - a felülvizsgálati napló egyedi bejegyzéseinek időbélyegei közötti kapcsolat tekintetében meghatározott tűréshatáron túli - időviszonyokat is tartalmazza.

3.3.12.12.3. Változtatások

Az elektronikus információs rendszer biztosítja a lehetőséget a meghatározott személyeknek vagy szerepköröknek arra, hogy megváltoztassák az egyes rendszerelemekre végrehajtandó naplózást a kiválasztott esemény kritériumok alapján, meghatározott időtartamon belül.

3.3.13. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

3.3.13.1. Rendszer- és kommunikációvédelmi eljárásrend

3.3.13.1.1. Az érintett szervezet:

3.3.13.1.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belüli szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a rendszer- és kommunikációvédelmi eljárásrendet, mely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

3.3.13.1.1.2. a rendszer- és kommunikációvédelmi eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a rendszer- és kommunikációvédelmére vonatkozó eljárásrendet.

3.3.13.2. Alkalmazás szétválasztás

Az elektronikus információs rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától.

3.3.13.3. Biztonsági funkciók elkülönítése

Az elektronikus információs rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.

3.3.13.4. Információmaradványok

Az elektronikus információs rendszer meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást.

3.3.13.5. Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem

Az elektronikus információs rendszer véd a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

3.3.13.6. A határok védelme

3.3.13.6.1. Az elektronikus információs rendszer:

3.3.13.6.1.1. felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt;

3.3.13.6.1.2. a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól;

3.3.13.6.1.3. csak az érintett szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

3.3.13.6.2. Hozzáférési pontok

Az érintett szervezet korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát.

3.3.13.6.3. Külső kommunikációs szolgáltatások

3.3.13.6.3.1. Az érintett szervezet:

3.3.13.6.3.1.1. felügyelt interfészt működtet minden külső infokommunikációs szolgáltatáshoz;

3.3.13.6.3.1.2. minden felügyelt interfészhez forgalomáramlási szabályokat alakít ki;

3.3.13.6.3.1.3. védi az összes interfésznél az átvitelre kerülő információk bizalmasságát és sértetlenségét;

3.3.13.6.3.1.4. dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együtt;

3.3.13.6.3.1.5. meghatározott gyakorisággal áttekinti a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol.

3.3.13.6.4. Alapeseti visszautasítás

Az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat.

3.3.13.6.5. Távoli készülékek megosztott csatornahasználatának tiltása

A távoli készülékkel kapcsolatban álló elektronikus információs rendszer meggátolja, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel.

3.3.13.6.6. Hitelesített proxy kiszolgálók

Az elektronikus információs rendszer hitelesített proxy - olyan szerver, számítógép vagy szerveralkalmazás, amely a kliensek kéréseit köztes elemként más szerverekhez továbbítja - kiszolgálók segítségével irányítja a belső kommunikációs forgalmat a felügyelt interfészeken a meghatározott külső hálózatokhoz.

3.3.13.6.7. Biztonsági hibaállapot

Az elektronikus információs rendszer hibaállapotba kerül a határvédelmi eszköz működési hibája esetén.

3.3.13.6.8. Rendszerelemek elkülönítése

Az érintett szervezet határvédelmi mechanizmusokat alkalmaz azoknak az elektronikus információs rendszerelemeknek az elkülönítésére, amelyek a meghatározott alapfeladatokat és alapfunkciókat támogatják.

3.3.13.7. Az adatátvitel bizalmassága

3.3.13.7.1. Az elektronikus információs rendszer védje meg a továbbított információk bizalmasságát.

3.3.13.7.2. Kriptográfiai vagy egyéb védelem

Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk jogosulatlan felfedése ellen, kivéve, ha az átvitel más, az érintett szervezet által meghatározott alternatív fizikai ellenintézkedéssel védett.

3.3.13.8. Az adatátvitel sértetlensége

3.3.13.8.1. Az elektronikus információs rendszer megvédi a továbbított információk sértetlenségét.

3.3.13.8.2. Kriptográfiai vagy egyéb védelem

Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve.

3.3.13.9. A hálózati kapcsolat megszakítása

Az elektronikus információs rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, meghatározott időtartamú inaktivitás után.

3.3.13.10. Kriptográfiai kulcs előállítása és kezelése

3.3.13.10.1. Az érintett szervezet előállítja és kezeli az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően.

3.3.13.10.2. Rendelkezésre állás

Az érintett szervezet előállítja, biztosítja az információk rendelkezésre állását abban az esetben is, amikor a kriptográfiai kulcsok elérhetetlenné válnak (elvesztés, sérülés, megsemmisülés).

3.3.13.11. Kriptográfiai védelem

Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

3.3.13.12. Együttműködésen alapuló számítástechnikai eszközök

Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

3.3.13.13. Nyilvános kulcsú infrastruktúra tanúsítványok

Az érintett szervezet nyilvános kulcsú tanúsítványokat állít ki a belső hitelesítési rend szerint, vagy a nyilvános kulcsú tanúsítványokat beszerzi a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatótól.

3.3.13.14. Mobilkód korlátozása

3.3.13.14.1. Az érintett szervezet:

3.3.13.14.1.1. meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat;

3.3.13.14.1.2. használati korlátozásokat vezet be vagy megvalósítási útmutatót bocsát ki az elfogadható mobilkódokra és mobilkód technológiákra;

3.3.13.14.1.3. engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az elektronikus információs rendszeren belül.

3.3.13.15. Elektronikus információs rendszeren keresztüli hangátvitel (úgynevezett VoIP)

3.3.13.15.1. Az érintett szervezet:

3.3.13.15.1.1. használati korlátozásokat vezet be vagy megvalósítási útmutatót ad a VoIP technológiákhoz, felmérve a rosszindulatú használat esetén az elektronikus információs rendszerben okozható károkat;

3.3.13.15.1.2. engedélyezi, felügyeli, és ellenőrzi a VoIP használatát az elektronikus információs rendszeren belül.

3.3.13.16. Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás)

Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód- és elődtartományok közötti bizalmi láncot.

3.3.13.17. Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás)

Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér, és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

3.3.13.18. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást egy szervezet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

3.3.13.19. Munkaszakasz hitelessége

Az elektronikus információs rendszer védje meg a munkaszakaszok hitelességét.

3.3.13.20. Hibát követő ismert állapot

Meghatározott hibatípusokhoz tartozó hibát követően az elektronikus információs rendszer a kijelölt, vagy utolsó ismert állapotba kerül, amely a hiba esetén is megőrzi a rendszerállapot információkat.

3.3.13.21. A maradvány információ védelme

Az elektronikus információs rendszer védi az érintett szervezet által meghatározott maradvány információk (pl.: átmeneti fájlok) bizalmasságát, sértetlenségét.

3.3.13.22. A folyamatok elkülönítése

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

2016/679 EURÓPAI PARLAMENT ÉS TANÁCS RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02016R0679-20160504&qid=1517231312658&from=HU

Általános rendelkezések

1. cikk

Tárgy

(1) Ez a rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg.

(2) Ez a rendelet a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.

(3) A személyes adatok Unión belüli szabad áramlása nem korlátozható vagy tiltható meg a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból.

2. cikk

Tárgyi hatály

(1) E rendeletet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

3. cikk

Területi hatály

(1) E rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem.

(2) E rendeletet kell alkalmazni az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:

a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy

b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.

(3) E rendeletet kell alkalmazni a személyes adatoknak a nem az Unióban, hanem olyan helyen tevékenységi hellyel rendelkező adatkezelő által végzett kezelésére, ahol a nemzetközi közjog értelmében valamely tagállam joga alkalmazandó.

4. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

2. „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

3. „az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

4. „profilalkotás”: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

5. „álnevesítés”: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

6. „nyilvántartási rendszer”: a személyes adatok bármely módon - centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint - tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

7. „adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

8. „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

9. „címzett”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

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

11. „az érintett hozzájárulása”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

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

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

14. „biometrikus adat”: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;

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

16. „tevékenységi központ”:

a) az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtatására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;

b) az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak;

17. „képviselő”: az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

18. „vállalkozás”: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;

19. „vállalkozáscsoport”: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;

20. „kötelező erejű vállalati szabályok”: a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;

21. „felügyeleti hatóság”: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv;

22. „érintett felügyeleti hatóság”: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;

b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy

c) panaszt nyújtottak be az említett felügyeleti hatósághoz;

23. „személyes adatok határokon átnyúló adatkezelése”:

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy

b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

24. „releváns és megalapozott kifogás”: a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;

25. „az információs társadalommal összefüggő szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv[1] 1. cikke (1) bekezdésének *b)* pontja értelmében vett szolgáltatás;

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

II. FEJEZET
Elvek

5. cikk
A személyes adatok kezelésére vonatkozó elvek

(1) A személyes adatok:

a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”);

b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztet-hetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhoz kötöttség”);

c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a

[1] Az Európai Parlament és Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról (HL L 241., 2015.9.17., 1. o.)

szükségesre kell korlátozódniuk („adattakarékosság”);

d) pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („pontosság”);

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („korlátozott tárolhatóság”);

f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

(2) Az adatkezelő felelős az (1) bekezdésnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

6. cikk
Az adatkezelés jogszerűsége

(1) A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Az első albekezdés *f)* pontja nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.

(2) Az e rendeletben foglalt, adatkezelésre vonatkozó szabályok alkalmazásának kiigazítása érdekében, a tagállamok az (1) bekezdés *c)* és *e)* pontjának való megfelelés céljából fenntarthatnak vagy bevezethetnek konkrétabb rendelkezéseket, amelyekben pontosabban meghatározzák az adatkezelésre vonatkozó konkrét követelményeket, és amelyekben további intézkedéseket tesznek az adatkezelés jogszerűségének és tisztességességének biztosítására, ideértve a IX. fejezetben meghatározott egyéb konkrét adatkezelési helyzeteket is.

(3) Az (1) bekezdés *c)* és *e)* pontja szerinti adatkezelés jogalapját a következőknek kell megállapítania:

a) az uniós jog, vagy
b) azon tagállami jog, amelynek hatálya alá az adatkezelő tartozik.

Az adatkezelés célját e jogalapra hivatkozással kell meghatározni, illetve az (1) bekezdés *e)* pontjában említett adatkezelés tekintetében annak szükségesnek kell lennie valamely közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához. Ez a jogalap tartalmazhat az e rendeletben foglalt szabályok alkalmazását kiigazító rendelkezéseket, ideértve az adatkezelő általi adatkezelés jogszerűségére irányadó általános feltételeket, az adatkezelés tárgyát képező adatok típusát, az érintetteket, azokat a jogalanyokat, amelyekkel a személyes adatok közölhetők, illetve az ilyen adatközlés céljait, az adatkezelés céljára vonatkozó korlátozásokat, az adattárolás időtartamát és az adatkezelési műveleteket, valamint egyéb adatkezelési eljárásokat, így a törvényes és tisztességes adatkezelés biztosításához szükséges intézkedéseket is, ideértve a IX. fejezetben meghatározott egyéb konkrét adatkezelési helyzetekre vonatkozóan. Az uniós vagy tagállami jognak közérdekű célt kell szolgálnia, és arányosnak kell lennie az elérni kívánt jogszerű céllal.

(4) Ha az adatgyűjtés céljától eltérő célból történő adatkezelés nem az érintett hozzájárulásán vagy valamely olyan uniós vagy tagállami jogon alapul, amely szükséges és arányos intézkedésnek minősül egy demokratikus társadalomban a 23. cikk (1) bekezdésében rögzített célok eléréséhez, annak megállapításához, hogy az eltérő célú adatkezelés összeegyeztethető-e azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték, az adatkezelő többek között figyelembe veszi:

a) a személyes adatok gyűjtésének céljait és a tervezett további adatkezelés céljai közötti esetleges kapcsolatokat;
b) a személyes adatok gyűjtésének körülményeit, különös tekintettel az érintettek és az adatkezelő közötti kapcsolatokra;
c) a személyes adatok jellegét, különösen pedig azt, hogy a 9. cikk szerinti személyes adatok különleges kategóriáinak kezeléséről van-e szó, illetve, hogy büntetőjogi felelősség megállapítására és bűncselekményekre vonatkozó adatoknak a 10. cikk szerinti kezeléséről van-e szó;

d) azt, hogy az érintettekre nézve milyen esetleges következményekkel járna az adatok tervezett további kezelése;

e) megfelelő garanciák meglétét, ami jelenthet titkosítást vagy álnevesítést is.

7. cikk
A hozzájárulás feltételei

(1) Ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.

(2) Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti e rendeletet, kötelező erővel nem bír.

(3) Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

(4) Annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, egyebek mellett, hogy a szerződés teljesítésének - beleértve a szolgáltatások nyújtását is - feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

III. FEJEZET
Az érintett jogai
1. szakasz
Átláthatóság és intézkedések

12. cikk
Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések

(1) Az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó, a 13. és a 14. cikkben említett valamennyi információt és a 15-22. és 34. cikk szerinti minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon

- ideértve adott esetben az elektronikus utat is - kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

(2) Az adatkezelő elősegíti az érintett 15-22. cikk szerinti jogainak a gyakorlását. A 11. cikk (2) bekezdésében említett esetekben az adatkezelő az érintett 15-22. cikk szerinti jogai gyakorlására irányuló kérelmének a teljesítését nem tagadhatja meg, kivéve, ha bizonyítja, hogy az érintettet nem áll módjában azonosítani.

(3) Az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a 15-22. cikk szerinti kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

(4) Ha az adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

(5) A 13. és 14. cikk szerinti információkat és a 15-22. és 34. cikk szerinti tájékoztatást és intézkedést díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy - különösen ismétlődő jellege miatt - túlzó, az adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:

a) észszerű összegű díjat számíthat fel, vagy
b) megtagadhatja a kérelem alapján történő intézkedést.

A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az adatkezelőt terheli.

(6) A 11. cikk sérelme nélkül, ha az adatkezelőnek megalapozott kétségei vannak a 15-21. cikk szerinti kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.

(7) Az érintett részére a 13. és 14. cikk alapján nyújtandó információkat szabványosított ikonokkal is ki lehet egészíteni annak érdekében, hogy a tervezett adatkezelésről az érintett jól látható, könnyen érthető és jól olvasható formában kapjon általános tájékoztatást. Az elektronikusan megjelenített ikonoknak géppel olvashatónak kell lenniük.

(8) A Bizottság felhatalmazást kap arra, hogy a 92. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el az ikonok által megjelenítendő információk és a szabványosított ikonok biztosítására vonatkozó eljárások meghatározása céljából.

2. szakasz
Tájékoztatás és a személyes adatokhoz való hozzáférés

13. cikk
Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik

(1) Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, az adatkezelő a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

a) az adatkezelőnek és - ha van ilyen - az adatkezelő képviselőjének a kiléte és elérhetőségei;
b) az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
d) a 6. cikk (1) bekezdésének *f)* pontján alapuló adatkezelés esetén, az adatkezelő vagy harmadik fél jogos érdekei;
e) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
f) adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a 46. cikkben, a 47. cikkben vagy a 49. cikk (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozás.

(2) Az (1) bekezdésben említett információk mellett az adatkezelő a személyes adatok megszerzésének időpontjában, annak érdekében, hogy a tisztességes és átlátható adatkezelést biztosítsa, az érintettet a következő kiegészítő információkról tájékoztatja:

a) a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
b) az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
c) a 6. cikk (1) bekezdésének *a)* pontján vagy a 9. cikk (2) bekezdésének *a)* pontján alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
d) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
e) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;

f) a 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

(3) Ha az adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és a (2) bekezdésben említett minden releváns kiegészítő információról.

(4) Az (1), (2) és (3) bekezdés nem alkalmazandó, ha és amilyen mértékben az érintett már rendelkezik az információkkal.

14. cikk

Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg

(1) Ha a személyes adatokat nem az érintettől szerezték meg, az adatkezelő az érintett rendelkezésére bocsátja a következő információkat:

a) az adatkezelőnek és - ha van ilyen - az adatkezelő képviselőjének a kiléte és elérhetőségei;
b) az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
d) az érintett személyes adatok kategóriái;
e) a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
f) adott esetben annak ténye, hogy az adatkezelő valamely harmadik országbeli címzett vagy valamely nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a 46. cikkben, a 47. cikkben vagy a 49. cikk (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az ezek másolatának megszerzésére szolgáló módokra vagy az elérhetőségükre való hivatkozás.

(2) Az (1) bekezdésben említett információk mellett az adatkezelő az érintett rendelkezésére bocsátja az érintettre nézve tisztességes és átlátható adatkezelés biztosításához szükséges következő kiegészítő információkat:

a) a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
b) ha az adatkezelés a 6. cikk (1) bekezdésének *f)* pontján alapul, az adatkezelő vagy harmadik fél jogos érdekeiről;
c) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat a személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való joga;

d) a 6. cikk (1) bekezdésének *a)* pontján vagy a 9. cikk (2) bekezdésének *a)* pontján alapuló adatkezelés esetén a hozzájárulás bármely időpontban való visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;

e) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;

f) a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e; és

g) a 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

(3) Az adatkezelő az (1) és (2) bekezdés szerinti tájékoztatást az alábbiak szerint adja meg:

a) a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül;

b) ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy

c) ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

(4) Ha az adatkezelő a személyes adatokon a megszerzésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és a (2) bekezdésben említett minden releváns kiegészítő információról.

(5) Az (1)-(4) bekezdést nem kell alkalmazni, ha és amilyen mértékben:

a) az érintett már rendelkezik az információkkal;

b) a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, a 89. cikk (1) bekezdésében foglalt feltételek és garanciák figyelembevételével végzett adatkezelés esetében, vagy amennyiben az e cikk (1) bekezdésében említett kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. Ilyen esetekben az adatkezelőnek megfelelő intézkedéseket kell hoznia - az információk nyilvánosan elérhetővé tételét is ideértve - az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;

c) az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik; vagy

d) a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia.

15. cikk

Az érintett hozzáférési joga

(1) Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;
b) az érintett személyes adatok kategóriái;
c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
h) a 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

(2) Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a 46. cikk szerinti megfelelő garanciákról.

(3) Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

(4) A (3) bekezdésben említett, másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

3. szakasz
Helyesbítés és törlés

16. cikk
A helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok - egyebek mellett kiegészítő nyilatkozat útján történő - kiegészítését.

17. cikk
A törléshez való jog („az elfeledtetéshez való jog”)

(1) Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az érintett visszavonja a 6. cikk (1) bekezdésének *a)* pontja vagy a 9. cikk (2) bekezdésének *a)* pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) az érintett a 21. cikk (1) bekezdése alapján tiltakozik az adatkezeléseó ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;

d) a személyes adatokat jogellenesen kezelték;

e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

f) a személyes adatok gyűjtésére a 8. cikk (1) bekezdésében említett, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

(2) Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és az (1) bekezdés értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket - ideértve technikai intézkedéseket - annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

(3) Az (1) és (2) bekezdés nem alkalmazandó, amennyiben az adatkezelés szükséges:

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

b) a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;

c) a 9. cikk (2) bekezdése *h)* és *i)* pontjának, valamint a 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján;

d) a 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az (1) bekezdésben említett jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy

e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

18. cikk

Az adatkezelés korlátozásához való jog

(1) Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;

b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d) az érintett a 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

(2) Ha az adatkezelés az (1) bekezdés alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

(3) Az adatkezelő az érintettet, akinek a kérésére az (1) bekezdés alapján korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

19. cikk

A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség

Az adatkezelő minden olyan címzettet tájékoztat a 16. cikk, a 17. cikk (1) bekezdése, illetve a 18. cikk szerinti valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

20. cikk

Az adathordozhatósághoz való jog

(1) Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

a) az adatkezelés a 6. cikk (1) bekezdésének *a)* pontja vagy a 9. cikk (2) bekezdésének *a)* pontja szerinti hozzájáruláson, vagy a 6. cikk (1) bekezdésének *b)* pontja szerinti szerződésen alapul; és

b) az adatkezelés automatizált módon történik.

(2) Az adatok hordozhatóságához való jog (1) bekezdés szerinti gyakorlása során az érintett jogosult arra, hogy - ha ez technikailag megvalósítható - kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

(3) Az e cikk (1) bekezdésében említett jog gyakorlása nem sértheti a 17. cikket. Az említett jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

(4) Az (1) bekezdésben említett jog nem érintheti hátrányosan mások jogait és szabadságait.

IV. FEJEZET
Az adatkezelő és az adatfeldolgozó
1. szakasz
Általános kötelezettségek

24. cikk
Az adatkezelő feladatai

(1) Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.

(2) Ha az az adatkezelési tevékenység vonatkozásában arányos, az (1) bekezdésben említett intézkedések részeként az adatkezelő megfelelő belső adatvédelmi szabályokat is alkalmaz.

(3) A 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozás felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti kötelezettségeit.

25. cikk
Beépített és alapértelmezett adatvédelem

(1) Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket - például álnevesítést - hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

(2) Az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

(3) A 42. cikk szerinti jóváhagyott tanúsítási mechanizmus felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti az e cikk (1) és (2) bekezdésében előírt követelményeket.

28. cikk

Az adatfeldolgozó

(1) Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

(2) Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

(3) Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan - az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó - szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben. A szerződés vagy más jogi aktus különösen előírja, hogy az adatfeldolgozó:

a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli - beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is -, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;

b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

c) meghozza a 32. cikkben előírt intézkedéseket;

d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan a (2) és (4) bekezdésben említett feltételeket;

e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett III. fejezetben foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

f) segíti az adatkezelőt a 32-36. cikk szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;

g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;

h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely az e cikkben meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az első albekezdés *h)* pontjával kapcsolatban az adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti ezt a rendeletet vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.

(4) Ha az adatfeldolgozó bizonyos, az adatkezelő nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozó szolgáltatásait is igénybe veszi, uniós vagy tagállami jog alapján létrejött szerződés vagy más jogi aktus útján erre a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött, a (3) bekezdésben említett szerződésben vagy egyéb jogi aktusban szerepelnek, különösen úgy, hogy a további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen e rendelet követelményeinek. Ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért.

(5) A 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozás felhasználható annak bizonyítása részeként, hogy az adatfeldolgozó biztosítja az (1) és (4) bekezdésben említett megfelelő garanciákat.

(6) Az adatkezelő és az adatfeldolgozó közötti egyedi szerződés sérelme nélkül az e cikk (3) és (4) bekezdésében említett szerződés vagy más jogi aktus teljes egészében vagy részben az e cikk (7) és (8) bekezdésében említett általános szerződési feltételeken alapulhat, beleértve azt is, amikor ezek a 42. és a 43. cikk alapján az adatkezelőnek vagy az adatfeldolgozónak megadott tanúsítvány részét képezik.

(7) A Bizottság - a 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárásnak megfelelően - általános szerződési feltételeket határozhat meg az e cikk (3) és (4) bekezdésében foglaltakra vonatkozóan.

(8) A felügyeleti hatóságok a 63. cikkben említett egységességi mechanizmusnak megfelelően általános szerződési feltételeket fogadhatnak el az e cikk (3) és (4) bekezdésében foglaltakra vonatkozóan.

(9) A (3) és (4) bekezdésben említett szerződést vagy más jogi aktust írásba kell foglalni, ideértve az elektronikus formátumot is.

(10) A 82., 83. és 84. cikk sérelme nélkül, ha egy adatfeldolgozó e rendeletet sértve maga határozza meg az adatkezelés céljait és eszközeit, akkor őt az adott adatkezelés tekintetében adatkezelőnek kell tekinteni.

29. cikk

Az adatkezelő vagy az adatfeldolgozó irányítása alatt végzett adatkezelés

Az adatfeldolgozó és bármely, az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag az adatkezelő utasításának megfelelően kezelheti, kivéve, ha az ettől való eltérésre őt uniós vagy tagállami jog kötelezi.

30. cikk

Az adatkezelési tevékenységek nyilvántartása

(1) Minden adatkezelő és - ha van ilyen - az adatkezelő képviselője a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet. E nyilvántartás a következő információkat tartalmazza:

a) az adatkezelő neve és elérhetősége, valamint - ha van ilyen - a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
b) az adatkezelés céljai;
c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
f) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;
g) ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

(2) Minden adatfeldolgozó és - ha van ilyen - az adatfeldolgozó képviselője nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról; a nyilvántartás a következő információkat tartalmazza:

a) az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá - ha van ilyen - az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;
b) az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;

c) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása;

d) ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

(3) Az (1) és (2) bekezdésben említett nyilvántartást írásban kell vezetni, ideértve az elektronikus formátumot is.

(4) Az adatkezelő vagy az adatfeldolgozó, valamint - ha van ilyen - az adatkezelő vagy az adatfeldolgozó képviselője megkeresés alapján a felügyeleti hatóság részére rendelkezésére bocsátja a nyilvántartást.

(5) Az (1) és (2) bekezdésben foglalt kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

Adatbiztonság

32. cikk
Az adatkezelés biztonsága

(1) Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

a) a személyes adatok álnevesítését és titkosítását;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

(2) A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

(3) Az adatkezelő, illetve az adatfeldolgozó 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozását felhasználhatja annak bizonyítása részeként, hogy az e cikk (1) bekezdésében meghatározott követelményeket teljesíti.

(4) Az adatkezelő és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

33. cikk

Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak

(1) Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

(2) Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

(3) Az (1) bekezdésben említett bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve - ha lehetséges - az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(4) Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

(5) Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.

34. cikk

Az érintett tájékoztatása az adatvédelmi incidensről

(1) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

(2) Az (1) bekezdésben említett, az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a 33. cikk (3) bekezdésének *b), c)* és *d)* pontjában említett információkat és intézkedéseket.

(3) Az érintettet nem kell az (1) bekezdésben említettek szerint tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket - mint például a titkosítás alkalmazása -, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

(4) Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a (3) bekezdésben említett feltételek valamelyikének teljesülését.

4. szakasz
Adatvédelmi tisztviselő

37. cikk
Az adatvédelmi tisztviselő kijelölése

(1) Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor:

a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;

b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé;

c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

(2) A vállalkozáscsoport közös adatvédelmi tisztviselőt is kijelölhet, ha az adatvédelmi tisztviselő valamennyi tevékenységi helyről könnyen elérhető.

(3) Ha az adatkezelő vagy az adatfeldolgozó közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv, közös adatvédelmi tisztviselő jelölhető ki több ilyen szerv számára, az adott szervek szervezeti felépítésének és méretének figyelembevételével.

(4) Az (1) bekezdésben foglaltaktól eltérő esetekben az adatkezelő vagy az adatfeldolgozó, illetve az adatkezelők vagy adatfeldolgozók kategóriáit képviselő egyesületek és egyéb szervezetek adatvédelmi tisztviselőt jelölhetnek ki, vagy ha ezt uniós vagy tagállami jog írja elő, kötelesek kijelölni. Az adatkezelőket vagy adatfeldolgozókat képviselő ilyen egyesületek és egyéb szervezetek nevében az adatvédelmi tisztviselő eljárhat.

(5) Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a 39. cikkben említett feladatok ellátására való alkalmasság alapján kell kijelölni.

(6) Az adatvédelmi tisztviselő az adatkezelő vagy az adatfeldolgozó alkalmazottja lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait.

(7) Az adatkezelő vagy az adatfeldolgozó közzéteszi az adatvédelmi tisztviselő nevét és elérhetőségét, és azokat a felügyeleti hatósággal közli.

38. cikk

Az adatvédelmi tisztviselő jogállása

(1) Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

(2) Az adatkezelő és az adatfeldolgozó támogatja az adatvédelmi tisztviselőt a 39. cikkben említett feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.

(3) Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel.

(4) Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.

(5) Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

(6) Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

39. cikk

Az adatvédelmi tisztviselő feladatai

(1) Az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

b) ellenőrzi az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését;

d) együttműködik a felügyeleti hatósággal; és

e) az adatkezeléssel összefüggő ügyekben - ideértve a 36. cikkben említett előzetes konzultációt is - kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

(2) Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

910/2014/EU európai parlamenti és tanácsi rendelet a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32014R0910&qid=1517229392296&from=HU

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

1. cikk
Tárgy

A belső piac megfelelő működésének biztosítása, ugyanakkor az elektronikus azonosító eszközök és a bizalmi szolgáltatások megfelelő szintű biztonságának garantálása érdekében ez a rendelet:

a) megállapítja azokat a feltételeket, amelyek mellett a tagállamok elismerik a természetes és jogi személyek más tagállamok bejelentett elektronikus azonosítási rendszerének keretébe tartozó elektronikus azonosító eszközeit;
b) megállapítja különösen az elektronikus tranzakciókhoz kapcsolódó bizalmi szolgáltatásokra vonatkozó szabályokat; valamint
c) létrehozza az elektronikus aláírások, az elektronikus bélyegzők, az elektronikus időbélyegzők, az elektronikus dokumentumok, az ajánlott elektronikus kézbesítési szolgáltatások és a weboldal-hitelesítési szolgáltatások jogi keretét.

2. cikk
Hatály

(1) Ez a rendelet a tagállamok által bejelentett elektronikus azonosítási rendszerekre és az Unió területén letelepedett bizalmi szolgáltatókra alkalmazandó.

(2) E rendelet nem alkalmazandó a nemzeti jogszabályokon vagy meghatározott résztvevők közötti megállapodásokon alapuló, kizárólag zárt rendszerekben alkalmazott bizalmi szolgáltatások nyújtására.

(3) E rendelet nem érinti a szerződések megkötésére és érvényességére, sem más, alaki követelményekkel kapcsolatos jogi vagy eljárási kötelezettségekre vonatkozó nemzeti vagy uniós jogot.

3. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „elektronikus azonosítás”: a természetes vagy jogi személyt, illetve jogi személyt képviselő természetes személyt egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata;

2. „elektronikus azonosító eszköz”: olyan hardver- és/vagy szoftvereszköz, amely a személyazonosító adatokat tartalmazza, és amelyet online szolgáltatások céljából történő azonosításra használnak;

3. „személyazonosító adat”: egy természetes vagy jogi személy vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő adat;

4. „elektronikus azonosítási rendszer”: elektronikus azonosításra alkalmas rendszer, amelynek keretében természetes vagy jogi személy, illetve egy jogi személyt képviselő természetes személy számára elektronikus azonosító eszközöket bocsátanak ki;

5. „hitelesítés”: olyan elektronikus folyamat, amely lehetővé teszi a természetes vagy jogi személy elektronikus azonosításának vagy az elektronikus adatok eredetének és sértetlenségének az igazolását;

6. „igénybe vevő fél”: olyan természetes vagy jogi személy, aki vagy amely elektronikus azonosítási vagy bizalmi szolgáltatást vesz igénybe;

7. „közigazgatási szerv”: az állam, a regionális vagy helyi hatóság, közjogi intézmény és egy vagy több ilyen hatóságból, illetve közjogi intézményből álló társulások vagy az említett hatóságok, szervek vagy társulások közül legalább egy által közszolgáltatások nyújtásával megbízott és e megbízásuk keretében eljáró magánjogi szervezetek;

8. „közjogi intézmény”: a 2014/24/EU európai parlamenti és tanácsi irányelv[2] 2. cikke (1) bekezdésének 4. pontjában meghatározott intézmény;

9. „aláíró”: elektronikus aláírást létrehozó természetes személy;

[2] Az Európai Parlament és a Tanács 2014. február 26-i 2014/24/EU irányelve a közbeszerzésről és a 2004/18/EK irányelv hatályon kívül helyezéséről (HL L 94., 2014.3.28., 65. o.).

10. „elektronikus aláírás”: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ;

11. „fokozott biztonságú elektronikus aláírás”: olyan elektronikus aláírás, amely megfelel az a 26. cikkben meghatározott követelményeknek;

12. „minősített elektronikus aláírás”: olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás minősített tanúsítványán alapul;

13. „elektronikus aláírás létrehozásához használt adat”: olyan egyedi adat, amelyet az aláíró elektronikus aláírás létrehozásához használ;

14. „elektronikus aláírás tanúsítványa”: olyan elektronikus igazolás, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez kapcsolja, és igazolja legalább az érintett személy nevét vagy álnevét;

15. „elektronikus aláírás minősített tanúsítványa”: olyan, elektronikus aláírás céljára használt tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel az I. mellékletben megállapított követelményeknek;

16. „bizalmi szolgáltatás”: rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások:

a) elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy
b) weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy
c) elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése;

17. „minősített bizalmi szolgáltatás”: olyan bizalmi szolgáltatás, amely megfelel az e rendeletben foglalt alkalmazandó követelményeknek;

18. „megfelelőségértékelő szervezet”: a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott szervezet, amelyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére;

19. „bizalmi szolgáltató”: egy vagy több bizalmi szolgáltatást nyújtó természetes vagy jogi személy; a bizalmi szolgáltató lehet minősített vagy nem minősített bizalmi szolgáltató;

20. „minősített bizalmi szolgáltató”: olyan bizalmi szolgáltató, amely egy vagy több minősített bizalmi szolgáltatást nyújt, és amelynek minősített státusát a felügyeleti szerv jóváhagyta;

21. „termék”: olyan hardver- vagy szoftvereszköz vagy ezek megfelelő része, amelyet bizalmi szolgáltatások nyújtásában való felhasználásra szántak;

22. „elektronikus aláírást létrehozó eszköz”: elektronikus aláírás létrehozására használt, konfigurált hardver- vagy szoftvereszköz;

23. „minősített elektronikus aláírást létrehozó eszköz”: olyan, elektronikus aláírást létrehozó eszköz, amely megfelel a II. mellékletben megállapított követelményeknek;

24. „bélyegző létrehozója”: elektronikus bélyegzőt létrehozó jogi személy;

25. „elektronikus bélyegző”: olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét;

26. „fokozott biztonságú elektronikus bélyegző”: olyan elektronikus bélyegző, amely megfelel a 36. cikkben meghatározott követelményeknek;

27. „minősített elektronikus bélyegző”: olyan, fokozott biztonságú elektronikus bélyegző, amelyet minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, és amely elektronikus bélyegző minősített tanúsítványán alapul;

28. „elektronikus bélyegző létrehozásához használt adatok”: olyan egyedi adatok, amelyeket az elektronikus bélyegző létrehozója elektronikus bélyegző létrehozásához használ;

29. „elektronikus bélyegző tanúsítványa”: olyan elektronikus tanúsítvány, amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja, és igazolja az érintett jogi személy nevét;

30. „elektronikus bélyegző minősített tanúsítványa”: elektronikus bélyegző olyan tanúsítványa, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a III. mellékletben megállapított követelményeknek;

31. „elektronikus bélyegzőt létrehozó eszköz”: elektronikus bélyegző létrehozására használt, konfigurált hardver- vagy szoftvereszköz;

32. „minősített elektronikus bélyegzőt létrehozó eszköz”: olyan, elektronikus bélyegzőt létrehozó eszköz, amely értelemszerűen megfelel a II. mellékletben megállapított követelményeknek;

33. „elektronikus időbélyegző”: olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban;

34. „minősített elektronikus időbélyegző”: olyan elektronikus időbélyegző, amely megfelel a 42. cikkben megállapított követelményeknek;

35. „elektronikus dokumentum”: elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom;

36. „ajánlott elektronikus kézbesítési szolgáltatás”: olyan szolgáltatás, amely lehetővé teszi az adatok harmadik felek közötti, elektronikus úton való továbbítását, és bizonyítékot szolgáltat a továbbított adatok kezelésére vonatkozóan, beleértve az adatok küldésének és fogadásának

igazolását, valamint amely védi a továbbított adatokat az adatvesztés, az adatlopás, az adatkárosodás vagy a jogosulatlan adatmódosítás kockázata ellen;

37. „minősített ajánlott elektronikus kézbesítési szolgáltatás”: olyan ajánlott elektronikus kézbesítési szolgáltatás, amely megfelel a 44. cikkben megállapított követelményeknek;

38. „weboldal-hitelesítő tanúsítvány”: olyan igazolás, amely lehetővé teszi a weboldal hitelesítését és a weboldalt ahhoz a természetes vagy jogi személyhez kapcsolja, akinek vagy amelynek részére a tanúsítványt kiállították;

39. „minősített weboldal-hitelesítő tanúsítvány”: olyan weboldal-hitelesítő tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel a IV. mellékletben megállapított követelményeknek;

40. „érvényesítési adatok”: elektronikus aláírás vagy elektronikus bélyegző érvényesítéséhez használt adatok;

41. „érvényesítés”: olyan folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus aláírás vagy bélyegző érvényes.

4. SZAKASZ

Elektronikus aláírás

25. cikk

Az elektronikus aláírás joghatása

(1) Az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.

(2) A minősített elektronikus aláírás a saját kezű aláírással azonos joghatású.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus aláírást az összes többi tagállamban el kell ismerni minősített elektronikus aláírásként.

26. cikk

A fokozott biztonságú elektronikus aláírásra vonatkozó követelmények

A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie:

a) kizárólag az aláíróhoz köthető;
b) alkalmas az aláíró azonosítására;
c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre,

amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;

d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

27. cikk

Elektronikus aláírások használata a közigazgatásban

(1) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához fokozott biztonságú elektronikus aláírás alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie azokat a fokozott biztonságú elektronikus aláírásokat, elektronikus aláírás minősített tanúsítványán alapuló, fokozott biztonságú elektronikus aláírásokat és minősített elektronikus aláírásokat, amelyeket legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy módszerek alkalmazásával hoztak létre.

(2) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához minősített tanúsítványon alapuló, fokozott biztonságú elektronikus aláírás alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie azokat a minősített tanúsítványon alapuló, fokozott biztonságú elektronikus aláírásokat és a minősített elektronikus aláírásokat, amelyeket legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy módszerek alkalmazásával hoztak létre.

(3) A közigazgatási szervek által nyújtott online szolgáltatások határokon átnyúló igénybevétele tekintetében a tagállamok nem követelhetnek meg a minősített elektronikus aláírásnál magasabb biztonsági szintű elektronikus aláírást.

(4) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a fokozott biztonságú elektronikus aláírásokra vonatkozó szabványok hivatkozási számainak listáját. Ha egy fokozott biztonságú elektronikus aláírás megfelel ezeknek a szabványoknak, vélelmezni kell, hogy az aláírás az e cikk (1) és (2) bekezdése és a 26. cikk szerinti, a fokozott biztonságú elektronikus aláírásokra vonatkozó követelményeket is teljesíti. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(5) 2015. szeptember 18-ig, és figyelembe véve a jelenlegi gyakorlatot, szabványokat és uniós jogi aktusokat, a Bizottság végrehajtási jogi aktusok útján meghatározza a fokozott biztonságú elektronikus aláírások referenciaformátumait, illetve az alternatív formátumok használata esetén alkalmazandó referencia-módszereket. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

28. cikk

Elektronikus aláírások minősített tanúsítványai

(1) Az elektronikus aláírások minősített tanúsítványainak meg kell felelniük az I. mellékletben foglalt követelményeknek.

(2) Az elektronikus aláírások minősített tanúsítványaira nem vonatkozhatnak olyan kötelező követelmények, amelyek az I. mellékletben foglalt előírásokat meghaladják.

(3) Az elektronikus aláírások minősített tanúsítványain további, nem kötelező jellegű egyedi jellemzőket is fel lehet tüntetni. Ezek a jellemzők nem érinthetik a minősített elektronikus aláírások interoperabilitását és elismerését.

(4) Ha az elektronikus aláírás minősített tanúsítványát a kezdeti aktiválást követően visszavonják, a tanúsítvány a visszavonás időpontjában érvényességét veszti, státusa pedig semmilyen körülmények között nem állítható vissza.

(5) A tagállamok az alábbi feltételek mellett nemzeti szabályokat határozhatnak meg az elektronikus aláírás minősített tanúsítványának ideiglenes felfüggesztésére vonatkozóan:

a) ha egy elektronikus aláírás minősített tanúsítványát ideiglenesen felfüggesztik, a tanúsítvány a felfüggesztés időtartamára érvényét veszti;

b) a felfüggesztés időtartamát egyértelműen fel kell tüntetni a tanúsítványok adatbázisában oly módon, hogy a felfüggesztett státus a felfüggesztés időtartama alatt látható legyen a tanúsítvány státusáról tájékoztatást nyújtó szolgáltatás igénybevétele során.

(6) A Bizottság végrehajtási jogi aktusok útján összeállíthatja az elektronikus aláírások minősített tanúsítványaira vonatkozó szabványok hivatkozási számainak listáját. Amennyiben az elektronikus aláírás minősített tanúsítványa megfelel ezeknek a szabványoknak, vélelmezni kell az I. mellékletben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

29. cikk

A minősített elektronikus aláírást létrehozó eszközökre vonatkozó követelmények

(1) A minősített elektronikus aláírást létrehozó eszközöknek meg kell felelniük a II. mellékletben foglalt követelményeknek.

(2) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a minősített elektronikus aláírást létrehozó eszközökre vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a minősített elektronikus aláírást létrehozó eszköz megfelel ezeknek a szabványoknak, vélelmezni kell a II. mellékletben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

30. cikk

A minősített elektronikus aláírást létrehozó eszközök tanúsítása

(1) A tagállamok által kijelölt megfelelő állami vagy magánszervek tanúsítják, hogy a minősített elektronikus aláírást létrehozó eszközök megfelelnek a II. mellékletben meghatározott követelményeknek.

(2) A tagállamok tájékoztatják a Bizottságot az (1) bekezdés alapján általuk kijelölt állami vagy magánszerv nevéről és címéről. A Bizottság ezt az információt a tagállamok rendelkezésére bocsátja.

(3) Az (1) bekezdésben említett tanúsításnak az alábbiak egyikén kell alapulnia:

a) biztonságértékelési eljárás, amelyet a második albekezdéssel összhangban létrehozott listán szereplő, információtechnológiai termékek biztonságának értékelésére vonatkozó szabványok egyikének megfelelően hajtottak végre.; vagy

b) az *a)* pontban említettől eltérő eljárás, feltéve, hogy összehasonlítható biztonsági szintet biztosít, és feltéve, hogy az (1) bekezdésben említett állami vagy magánszerv értesítette a Bizottságot erről az eljárásról. Ez az eljárás csak az *a)* pontban említett szabványok hiányában alkalmazható, vagy akkor, ha az *a)* pontban említett biztonságértékelési eljárás folyamatban van.

A Bizottság végrehajtási jogi aktusok útján létrehozza az *a)* pontban említett információtechnológiai termékek biztonságának értékelésére vonatkozó szabványok listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni

(4) A Bizottság felhatalmazást kap arra, hogy a 47. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el az e cikk (1) bekezdésében említett kijelölt szervek által teljesítendő részletes feltételek meghatározása céljából.

31. cikk

A minősített elektronikus aláírást létrehozó tanúsított eszközök listájának közzététele

(1) A tagállamok indokolatlan késedelem nélkül, de legkésőbb egy hónappal a tanúsítás lezárultát követően bejelentik a Bizottságnak a 30. cikk (1) bekezdésében említett szervek által tanúsított, minősített elektronikus aláírást létrehozó eszközökre vonatkozó adatokat. A tagállamok kötelesek továbbá indokolatlan késedelem nélkül, de legkésőbb egy hónappal a tanúsítás visszavonását követően bejelenteni a Bizottságnak a tanúsítvánnyal már nem rendelkező, elektronikus aláírást létrehozó eszközökre vonatkozó adatokat.

(2) A beérkezett adatok alapján a Bizottság összeállítja, közzéteszi és fenntartja a, minősített elektronikus aláírást létrehozó tanúsított eszközök listáját.

(3) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az (1) bekezdés céljából alkalmazandó formátumokat és eljárásokat. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

32. cikk

A minősített elektronikus aláírás érvényesítésére vonatkozó követelmények

(1) A minősített elektronikus aláírás érvényesítésére szolgáló eljárás megállapítja a minősített elektronikus aláírás érvényességét, amennyiben:

a) az aláírást igazoló tanúsítvány az aláírás időpontjában elektronikus aláírás olyan minősített tanúsítványa volt, amely megfelel az I. mellékletnek;
b) a minősített tanúsítványt minősített bizalmi szolgáltató bocsátotta ki, és az az aláírás időpontjában érvényes volt;
c) az aláírás-érvényesítési adatok megfelelnek a szolgáltatást igénybe vevő fél számára megadott adatoknak;
d) a szolgáltatást igénybe vevő fél pontosan megkapja a tanúsítványban az aláírót azonosító egyedi adatokat;
e) amennyiben az aláírás időpontjában álnév használatára került sor, az álnév használatának tényét egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;
f) az elektronikus aláírást minősített elektronikus aláírást létrehozó eszközzel állították elő;
g) az aláírt adatok sértetlensége nem került veszélybe;
h) az aláírás időpontjában teljesültek a 26. cikkben foglalt követelmények;

(2) A minősített elektronikus aláírás érvényesítésére használt rendszernek biztosítania kell az érvényesítési eljárás pontos eredményét a szolgáltatást igénybe vevő fél számára, és lehetővé kell tennie, hogy a szolgáltatást igénybe vevő fél minden, a biztonságot érintő problémát észleljen.

(3) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a minősített elektronikus aláírások érvényesítésére vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a minősített elektronikus aláírás érvényesítése megfelel ezeknek a szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

33. cikk

Minősített elektronikus aláírást érvényesítő minősített érvényesítési szolgáltatás

(1) Minősített elektronikus aláírást érvényesítő minősített érvényesítési szolgáltatást kizárólag olyan minősített bizalmi szolgáltató nyújthat, amely:

a) a 32. cikk (1) bekezdésének megfelelő érvényesítést biztosít; és
b) lehetővé teszi a szolgáltatást igénybe vevő felek részére, hogy olyan automatizált módon kapják meg az érvényesítési eljárás eredményét, amely megbízható és hatékony, és amelyet

a minősített érvényesítési szolgáltatás biztosítójának fokozott biztonságú elektronikus aláírásával vagy fokozott biztonságú elektronikus bélyegzőjével láttak el.

(2) A Bizottság végrehajtási jogi aktusok útján összeállíthatja az (1) bekezdésben említett minősített érvényesítési szolgáltatásra vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a minősített elektronikus aláírást érvényesítő szolgáltatás megfelel ezeknek a szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

5. SZAKASZ

Elektronikus bélyegzők

35. cikk
Az elektronikus bélyegző joghatása

(1) Az elektronikus bélyegző joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formában létezik, illetve nem felel meg a minősített elektronikus bélyegzőkre vonatkozó követelményeknek.

(2) A minősített elektronikus bélyegzők esetében vélelmezni kell a hozzájuk kapcsolódó adatok sértetlenségét és a bélyegzőnek megfelelő eredetét.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus bélyegzőt valamennyi tagállamban el kell ismerni minősített elektronikus bélyegzőként.

36. cikk
Fokozott biztonságú elektronikus bélyegzőkre vonatkozó követelmények

A fokozott biztonságú elektronikus bélyegzőnek az alábbi követelményeknek kell megfelelnie:

a) kizárólag a bélyegző létrehozójához kötött;
b) alkalmas a bélyegző létrehozójának azonosítására;
c) olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozzák létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat;
d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása nyomon követhető;

37. cikk

Elektronikus bélyegzők használata a közigazgatásban

(1) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához fokozott biztonságú elektronikus bélyegző alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy az ott említett módszerek alkalmazásával létrehozott fokozott biztonságú elektronikus bélyegzőket, elektronikus bélyegzők minősített tanúsítványain alapuló, fokozott biztonságú elektronikus bélyegzőket és minősített elektronikus bélyegzőket.

(2) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához elektronikus bélyegző minősített tanúsítványán alapuló, fokozott biztonságú elektronikus bélyegző alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie az elektronikus bélyegző minősített tanúsítványán alapuló, fokozott biztonságú elektronikus bélyegzőket és a minősített elektronikus bélyegzőket legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy alkalmazási módszerekben.

(3) A közigazgatási szervek által nyújtott online szolgáltatások határokon átnyúló igénybevétele tekintetében a tagállamok nem követelhetnek meg a minősített elektronikus bélyegzőnél magasabb biztonsági szintű elektronikus bélyegzőt.

(4) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a fokozott biztonságú elektronikus bélyegzőkre vonatkozó szabványok hivatkozási számainak listáját. Ha egy fokozott biztonságú elektronikus bélyegző megfelel ezeknek a szabványoknak, vélelmezni kell, hogy a bélyegző az e cikk (1) és (2) bekezdése és a 36. cikk szerinti, a fokozott biztonságú elektronikus bélyegzőkre vonatkozó követelményeket is teljesíti. Az említett végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(5) 2015. szeptember 18-ig, és figyelembe véve a jelenlegi gyakorlatot, szabványokat és az Unió jogi aktusait, a Bizottság végrehajtási jogi aktusok útján meghatározza a fokozott biztonságú elektronikus bélyegzők referenciaformátumait, illetve az alternatív formátumok használata esetén alkalmazandó referencia-módszereket. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

38. cikk

Elektronikus bélyegzők minősített tanúsítványai

(1) Az elektronikus bélyegzők minősített tanúsítványainak meg kell felelniük a III. mellékletben foglalt követelményeknek.

(2) Az elektronikus bélyegzők minősített tanúsítványaira nem vonatkozhatnak olyan kötelező követelmények, amelyek a III. mellékletben foglalt előírásokat meghaladják.

(3) Az elektronikus bélyegzők minősített tanúsítványain további, nem kötelező jellegű egyedi jellemzők is feltüntethetők. Ezek a jellemzők nem érinthetik a minősített elektronikus bélyegzők interoperabilitását és elismerését.

(4) Ha az elektronikus bélyegző minősített tanúsítványát a kezdeti aktiválást követően visszavonják, a tanúsítvány a visszavonás időpontjában érvényét veszti, státusa pedig semmilyen körülmények között nem állítható vissza.

(5) A tagállamok az alábbi feltételek mellett nemzeti szabályokat határozhatnak meg az elektronikus bélyegzők minősített tanúsítványai ideiglenes felfüggesztésére vonatkozóan:

a) ha egy elektronikus bélyegző minősített tanúsítványát ideiglenesen felfüggesztik, a tanúsítvány a felfüggesztés időtartamára érvényét veszti;

b) a felfüggesztés időtartamát egyértelműen fel kell tüntetni a tanúsítványok adatbázisában oly módon, hogy a felfüggesztett státus a felfüggesztés időtartama alatt látható legyen a tanúsítvány státusáról tájékoztatást nyújtó szolgáltatás igénybevétele során.

(6) A Bizottság végrehajtási jogi aktusok útján összeállíthatja az elektronikus bélyegzők minősített tanúsítványaira vonatkozó szabványok hivatkozási számainak listáját. Amennyiben az elektronikus bélyegző minősített tanúsítványa megfelel ezeknek a szabványoknak, vélelmezni kell a III. mellékletben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

39. cikk

Minősített elektronikus bélyegzőt létrehozó eszközök

(1) A 29. cikket értelemszerűen alkalmazni kell a minősített elektronikus bélyegzőt létrehozó eszközökre vonatkozó követelményekre.

(2) A 30. cikket értelemszerűen alkalmazni kell a minősített elektronikus bélyegzőt létrehozó eszközök tanúsítására.

(3) A 31. cikket értelemszerűen alkalmazni kell a tanúsított, minősített elektronikus bélyegzőt létrehozó eszközök listájának közzétételére.

40. cikk

A minősített elektronikus bélyegzők érvényesítése és megőrzése

A 32., 33. és 34. cikket értelemszerűen alkalmazni kell a minősített elektronikus bélyegzők érvényesítésére és megőrzésére.

6. SZAKASZ

Elektronikus időbélyegző

41. cikk
Az elektronikus időbélyegző joghatása

(1) Az elektronikus időbélyegző joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus időbélyegzőkre vonatkozó követelményeknek.

(2) A minősített elektronikus időbélyegző esetében vélelmezni kell az általa feltüntetett dátum és időpont pontosságát, valamint az adott dátumhoz és időponthoz kapcsolt adatok sértetlenségét.

(3) Valamely tagállamban kibocsátott minősített elektronikus időbélyegzőt valamennyi tagállamban el kell ismerni minősített elektronikus időbélyegzőként.

42. cikk
A minősített elektronikus időbélyegzőre vonatkozó követelmények

(1) A minősített elektronikus időbélyegzőnek az alábbi követelményeknek kell megfelelnie:

a) az adatokat oly módon kell a dátumhoz és az időponthoz kapcsolnia, hogy az ésszerű mértékben kizárja az adatok észrevétlen megváltoztatásának lehetőségét;
b) az egyezményes koordinált világidőhöz kötött pontos időforráson kell alapulnia; és
c) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírásával vagy fokozott biztonságú elektronikus bélyegzőjével, vagy más egyenértékű módszerrel kell ellenjegyezni.

(2) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a dátumnak és az időpontnak az adatokhoz való hozzárendelésére, valamint a pontos időforrásokra vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a dátumnak és az időpontnak az adatokhoz való hozzárendelése, valamint a pontos időforrás megfelel ezeknek a szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

IV. FEJEZET
ELEKTRONIKUS DOKUMENTUMOK

46. cikk
Az elektronikus dokumentum joghatása

Az elektronikus dokumentum joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú.

I. MELLÉKLET

AZ ELEKTRONIKUS ALÁÍRÁSOK MINŐSÍTETT TANÚSÍTVÁNYAIRA VONATKOZÓ KÖVETELMÉNYEK

Az elektronikus aláírások minősített tanúsítványainak a következőket kell tartalmazniuk:

a) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt elektronikus aláírás minősített tanúsítványaként bocsátották ki;

b) a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatót egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett szolgáltató letelepedett, valamint
- jogi személy esetében a hivatalos nyilvántartásban szereplő megnevezést és adott esetben nyilvántartási számot,
- természetes személy esetében a személy nevét;

c) legalább az aláíró neve vagy pedig egy álnév;. álnév használata esetén ezt egyértelműen jelezni kell;

d) az elektronikus aláírás érvényesítéséhez használt adat, amely megfelel az elektronikus aláírás létrehozásához használt adatnak;

e) a tanúsítvány érvényességi idejének kezdete és vége;

f) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie;

g) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírása vagy fokozott biztonságú elektronikus bélyegzője;

h) az a helyszín, ahol a *g)* pontban említett, a fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;

i) azoknak a szolgáltatásoknak a helye, amelyek segítségével felvilágosítás kérhető a minősített tanúsítvány érvényességi állapotáról;

j) amennyiben az elektronikus aláírás érvényesítéséhez használt adathoz kapcsolódó, elektronikus aláírás létrehozásához használt adat minősített elektronikus aláírást létrehozó eszközön található, ennek megfelelő feltüntetése, legalább automatizált feldolgozásra alkalmas formában.

II. MELLÉKLET

A MINŐSÍTETT ELEKTRONIKUS ALÁÍRÁST LÉTREHOZÓ ESZKÖZÖKRE VONATKOZÓ KÖVETELMÉNYEK

1. A minősített elektronikus aláírást létrehozó eszközöknek megfelelő technikai és eljárási megoldások segítségével garantálniuk kell legalább azt, hogy:

a) az elektronikus aláírás létrehozásához használt adat bizalmassága ésszerű mértékben biztosítva legyen;

b) az elektronikus aláírás létrehozásához használt adat gyakorlatilag csak egyszer jöhessen létre;

c) az elektronikus aláírás létrehozásához használt adatok kikövetkeztethetősége ésszerű mértékig kizárható legyen, az elektronikus aláírás pedig megbízhatóan védve legyen a jelenleg rendelkezésre álló technológiákkal elkövetett hamisítás ellen;

d) az elektronikus aláírás létrehozásához használt adatot a jogszerűen aláíró személy megbízható védelemmel tudja ellátni a mások általi felhasználás ellen.

2. A minősített elektronikus aláírást létrehozó eszközök nem módosíthatják az aláírással ellátandó adatokat, és nem akadályozhatják meg, hogy az adatokat az aláíró az aláírás előtt megtekintse.

3. Az elektronikus aláírás létrehozásához használt adatnak az aláíró nevében történő előállítását és kezelését csak minősített bizalmi szolgáltató végezheti.

4. Az 1. pont *d)* alpontjának sérelme nélkül, az elektronikus aláírás létrehozásához használt adat kezelését az aláíró nevében végző minősített bizalmi szolgáltatók kizárólag adatmentési célból biztonsági másolatot készíthetnek az elektronikus aláírás létrehozásához használt adatról, amennyiben teljesülnek a következő követelmények:

a) a biztonsági adatállomány ugyanolyan biztonságos, mint az eredeti adatállomány;

b) a biztonsági adatállományok száma nem haladhatja meg a szolgáltatás folytonosságának biztosításához minimálisan szükséges mennyiséget.

III. MELLÉKLET

AZ ELEKTRONIKUS BÉLYEGZŐK MINŐSÍTETT TANÚSÍTVÁNYAIRA VONATKOZÓ KÖVETELMÉNYEK

Az elektronikus bélyegzők minősített tanúsítványainak a következőket kell tartalmazniuk:

a) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt elektronikus bélyegző minősített tanúsítványaként bocsátották ki;

b) a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatót egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett szolgáltató letelepedett és
- jogi személy esetében a hivatalos nyilvántartásban szereplő megnevezést és adott esetben nyilvántartási számot,
- természetes személy esetében a személy nevét;

c) a bélyegző létrehozójának legalább a hivatalos nyilvántartásban szereplő neve és adott esetben nyilvántartási száma;

d) az elektronikus bélyegző érvényesítéséhez használt adat, amelyek megfelel az elektronikus bélyegző létrehozásához használt adatnak;

e) a tanúsítvány érvényességi idejének kezdete és vége;

f) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie;

g) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírása vagy fokozott biztonságú elektronikus bélyegzője;

h) az a helyszín, ahol a *g)* pontban említett, a fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;

i) azoknak a szolgáltatásoknak a helye, amelyek segítségével felvilágosítás kérhető a minősített tanúsítvány érvényességi állapotáról;

j) amennyiben az elektronikus bélyegző érvényesítéséhez használt adathoz kapcsolódó, elektronikus bélyegző létrehozásához használt adat minősített elektronikus bélyegzőt létrehozó eszközön található, ennek megfelelő feltüntetése, legalább automatizált feldolgozásra alkalmas formában.

2015/1505 BIZOTTSÁG (EU) VÉGREHAJTÁSI HATÁROZATA a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 22. cikkének (5) bekezdése szerinti bizalmi listákhoz kapcsolódó technikai specifikációk és formátumok meghatározásáról

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32015D1505&qid=1517230687449&from=HU

1. cikk

A tagállamok bizalmi listát hoznak létre, tartanak fenn és tesznek közzé, amelyben szerepelnek a felügyeletük alá tartozó minősített bizalmi szolgáltatókra vonatkozó információk, valamint az e szolgáltatók által nyújtott minősített bizalmi szolgáltatásokra vonatkozó információk. E listának meg kell felelnie az I. mellékletben található technikai specifikációnak.

2. cikk

A tagállamok a bizalmi listában szerepeltethetnek adatokat a nem minősített bizalmi szolgáltatókról és az általuk nyújtott nem minősített bizalmi szolgáltatásokról. A listában egyértelműen jelezni kell, hogy mely bizalmi szolgáltatók és mely bizalmi szolgáltatásaik nem minősítettek.

3. cikk

(1) A 910/2014/EU rendelet 22. cikkének (2) bekezdése értelmében a tagállamok az I. mellékletben megadott technikai specifikációnak megfelelően elektronikus aláírással vagy bélyegzővel látják el bizalmi listájuk automatizált feldolgozásra alkalmas változatát.

(2) Amennyiben egy tagállam a bizalmi lista emberi által olvasható változatát is elektronikusan közzéteszi, gondoskodnia kell arról, hogy a bizalmi lista ezen változata ugyanazokat az adatokat tartalmazza, mint az automatizált feldolgozásra alkalmas változat, és azt a tagállamnak elektronikus aláírással vagy bélyegzővel kell ellátnia az I. mellékletben ismertetett technikai specifikációnak megfelelően.

4. cikk

(1) A tagállamok a II. mellékletben található sablon alkalmazásával bejelentik a Bizottságnak a 910/2014/EU rendelet 22. cikkének (3) bekezdésében említett adatokat.

(2) Az (1) bekezdésben említett adatok kettő vagy több rendszerüzemeltető legalább három hónapos, elcsúsztatott érvényességi időszakokkal rendelkező nyilvános kulcsú tanúsítványát jelentik, amely kulcsok megfelelnek a bizalmi lista automatizált feldolgozásra alkalmas változatának és ember által olvasható változatának elektronikus aláírására és elektronikus bélyegzővel való ellátására felhasználható titkos kulcsoknak, amikor azokat közzéteszik.

(3) A Bizottság a 910/2014/EU rendelet 22. cikkének (4) bekezdése értelmében biztonságos csatornán keresztül egy hitelesített webszerveren, automatizált feldolgozásra alkalmas, aláírással vagy bélyegzővel ellátott formátumban elérhetővé teszi a nyilvánosság számára az (1) és (2) bekezdésben említett adatokat, ahogy azokat a tagállamok bejelentik.

(4) A Bizottság biztonságos csatornán keresztül, egy hitelesített webszerveren, ember által olvasható, aláírással vagy bélyegzővel ellátott formátumban elérhetővé teheti a nyilvánosság számára az (1) és (2) bekezdésben említett adatokat, ahogy azokat a tagállamok bejelentik.

I. MELLÉKLET

TECHNIKAI SPECIFIKÁCIÓK A BIZALMI LISTÁK EGYSÉGES SABLONJÁHOZ

I. FEJEZET
ÁLTALÁNOS KÖVETELMÉNYEK

A bizalmi lista tartalmazza mind a jelenlegi, mind pedig a korábbi információkat a felsorolt bizalmi szolgáltatások státusáról attól az időponttól kezdve, amikor a bizalmi szolgáltatót felvették a bizalmi listákra.

Ezen specifikációban a „jóváhagyott”, „akkreditált” és/vagy „felügyelt” kifejezések magukban foglalják a nemzeti jóváhagyási rendszereket is, de a nemzeti jóváhagyási rendszerekkel kapcsolatban a bizalmi szolgáltatók nemzeti listájában a tagállamok további információkat fognak közölni, többek között a minősített bizalmi szolgáltatókra és az általuk biztosított bizalmi szolgáltatásokra alkalmazott felügyeleti rendszerekhez viszonyított esetleges eltérésekre vonatkozóan is.

A bizalmi listában szereplő információk elsődleges célja a minősített bizalmiszolgáltatás-tokenek, azaz a bizalmi szolgáltatások igénybe vételének eredményeként generált vagy kiállított fizikai vagy bináris (logikai) objektumok, pl. a minősített elektronikus aláírások/bélyegzők, minősített tanúsítvánnyal kísért fokozott biztonságú elektronikus aláírások/ bélyegzők, minősített időbélyegzők, minősített elektronikus kézbesítési igazolások stb. érvényessége ellenőrzésének támogatása.

II. FEJEZET
A BIZALMI LISTÁK EGYSÉGES SABLONJÁNAK RÉSZLETES SPECIFIKÁCIÓJA

Ez a specifikáció az ETSI TS 119 612 v2.1.1. szabványban (a továbbiakban: ETSI TS 119 612 szabvány) szereplő specifikációkon és követelményeken alapul.

Amennyiben e specifikáció külön követelményt nem tartalmaz, teljes mértékben az ETSI TS 119 612 szabvány 5. és 6. pontját kell alkalmazni. Amennyiben e specifikáció külön követelményeket tartalmaz, ezek elsőbbséget élveznek az ETSI TS 119 612 szabvány vonatkozó követelményeivel szemben. A e specifikáció és az ETSI TS 119 612 szabvány specifikációja közötti ütközés esetén ez a specifikáció az irányadó.

2015/1506 BIZOTTSÁG (EU) VÉGREHAJTÁSI HATÁROZATA a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 27. cikkének (5) bekezdése és 37. cikkének (5) bekezdése szerint a közigazgatási szervek által elismert fokozott biztonságú elektronikus aláírások és fokozott biztonságú bélyegzők formátumaira vonatkozó specifikációk meghatározásáról

http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32015D1505&qid=1517230687449&from=HU

1. cikk

A 910/2014/EU rendelet 27. cikkének (1) és (2) bekezdése szerint fokozott biztonságú elektronikus aláírást vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást előíró tagállamok elismerik az XML, CMS és PDF formátumú, B, T vagy LT megfelelőségi szintű fokozott biztonságú elektronikus aláírásokat, valamint a kapcsolódó aláírás-konténert tartalmazó fokozott biztonságú elektronikus aláírásokat, amennyiben az aláírások megfelelnek a mellékletben foglalt technikai specifikációnak.

2. cikk

(1) A 910/2014/EU rendelet 27. cikkének (1) és (2) bekezdése szerint fokozott biztonságú elektronikus aláírást vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírást előíró tagállamok elismernek az e határozat 1. cikkében említett elektronikus aláírás-formátumoktól eltérő formátumokat is, feltéve, hogy az aláíró által igénybe vett bizalmi szolgáltató székhelye szerinti tagállam más tagállamoknak aláírás-hitelesítési lehetőségeket kínál, amelyek lehetőség szerint alkalmasak automatizált feldolgozásra.

(2) Az aláírás-hitelesítési lehetőségeknek:

a) lehetővé kell tenniük a tagállamok számára, hogy online, ingyenesen és a nyelvet nem beszélők számára is érthetően hitelesítsék a kapott elektronikus aláírásokat;

b) meg kell jelenniük az aláírt dokumentumban, az elektronikus aláírásban vagy az elektronikus dokumentumkonténerben; és

c) igazolniuk kell a fokozott biztonságú elektronikus aláírás hitelességét, amennyiben:

1. a fokozott biztonságú elektronikus aláírást alátámasztó tanúsítvány érvényes volt az aláírás időpontjában, és ha a fokozott biztonságú elektronikus aláírást minősített tanúsítvány támasztja alá, akkor a fokozott biztonságú elektronikus aláírást alátámasztó minősített tanúsítvány az aláírás időpontjában egy olyan, elektronikus aláírásokra vonatkozó minősített tanúsítvány volt, amely megfelel a 910/2014/EU rendelet I. mellékletének, és egy minősített bizalmi szolgáltató adta ki azt;

2. az aláírás-hitelesítési adatok megfelelnek a szolgáltatást igénybe vevő fél számára megadott adatoknak;

3. a szolgáltatást igénybe vevő fél pontosan megkapja az aláírót egyedi módon azonosító adatokat;

4. amennyiben az aláírás időpontjában álnév használatára került sor, az álnév használatának tényét egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;

5. ha a fokozott biztonságú elektronikus aláírást minősített elektronikus aláírást létrehozó eszközzel állítottak elő, bármely ilyen eszköz használatát egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;

6. az aláírt adatok sértetlensége nem került veszélybe;

7. az aláírás időpontjában teljesültek a 910/2014/EU rendelet 26. cikkében foglalt követelmények;

8. a fokozott biztonságú elektronikus aláírás hitelesítésére használt rendszer biztosítja a hitelesítési eljárás pontos eredményét a szolgáltatást igénybe vevő fél számára, és lehetővé teszi, hogy a szolgáltatást igénybe vevő fél minden, a biztonságot érintő problémát észleljen.

3. cikk

A 910/2014/EU rendelet 37. cikkének (1) és (2) bekezdése szerint fokozott biztonságú elektronikus bélyegzőt vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzőt előíró tagállamok elismerik az XML, CMS és PDF formátumú, B, T vagy LT megfelelőségi szintű fokozott biztonságú elektronikus bélyegzőket, valamint a kapcsolódó aláírás-konténert tartalmazó fokozott biztonságú elektronikus bélyegzőket, amennyiben a bélyegzők megfelelnek a mellékletben foglalt technikai specifikációnak.

4. cikk

(1) A 910/2014/EU rendelet 37. cikkének (1) és (2) bekezdése szerint fokozott biztonságú elektronikus bélyegzőt vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzőt előíró tagállamok elismerik az e határozat 3. cikkében említett elektronikus bélyegzőformátumoktól eltérő formátumokat is, feltéve, hogy a bélyegző létrehozója által igénybe vett bizalmi szolgáltató székhelye szerinti tagállam más tagállamoknak bélyegzőhitelesítési lehetőségeket kínál, amelyek lehetőség szerint alkalmasak automatizált feldolgozásra.

(2) A bélyegzőhitelesítési lehetőségeknek:

a) lehetővé kell tenniük a tagállamok számára, hogy online, ingyenesen és a nyelvet nem beszélők számára is érthetően hitelesítsék a kapott elektronikus bélyegzőket;

b) meg kell jelenniük a bélyegzővel ellátott dokumentumban, az elektronikus bélyegzőben vagy az elektronikus dokumentumkonténerben;

c) igazolniuk kell a fokozott biztonságú elektronikus bélyegző hitelességét, amennyiben:

1. a fokozott biztonságú elektronikus bélyegzőt alátámasztó tanúsítvány érvényes volt a bélyegzés időpontjában, és ha a fokozott biztonságú elektronikus bélyegzőt minősített tanúsítvány támasztja alá, akkor a fokozott biztonságú elektronikus bélyegzőt alátámasztó minősített tanúsítvány a bélyegzés időpontjában egy olyan, elektronikus bélyegzőkre vonatkozó minősített tanúsítvány volt, amely megfelel a 910/2014/EU rendelet III. mellékletének, és egy minősített bizalmi szolgáltató adta ki azt;

2. a bélyegzőhitelesítési adatok megfelelnek a szolgáltatást igénybe vevő fél számára megadott adatoknak;

3. a szolgáltatást igénybe vevő fél pontosan megkapja a bélyegző létrehozóját egyedi módon azonosító adatokat;

4. amennyiben a bélyegzés időpontjában álnév használatára került sor, az álnév használatának tényét egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;

5. ha a fokozott biztonságú elektronikus bélyegzőt minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, bármely ilyen eszköz használatát egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;

6. a bélyegzővel ellátott adatok sértetlensége nem került veszélybe;

7. a bélyegzés időpontjában teljesültek a 910/2014/EU rendelet 36. cikkében foglalt követelmények;

8. a fokozott biztonságú elektronikus bélyegző hitelesítésére használt rendszer biztosítja a hitelesítési eljárás pontos eredményét a szolgáltatást igénybe vevő fél számára, és lehetővé teszi, hogy a szolgáltatást igénybe vevő fél minden, a biztonságot érintő problémát észleljen.

MELLÉKLET

Az XML, CMS és PDF formátumú, fokozott biztonságú elektronikus aláírásokra és a kapcsolódó aláíráskonténerre vonatkozó technikai specifikációk jegyzéke

A határozat 1. cikkében említett fokozott biztonságú elektronikus aláírásoknak meg kell felelniük az alábbi ETSI technikai specifikációk egyikének, kivéve azok 9. pontját:

XAdES alapprofil	ETSI TS 103171 v.2.1.1. (1)
CAdES alapprofil	ETSI TS 103173 v.2.2.1. (2)
PAdES alapprofil	ETSI TS 103172 v.2.2.2. (3)

(1) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
(2) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
(3) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

A határozat 1. cikkében említett kapcsolódó aláírás-konténernek meg kell felelnie az alábbi ETSI technikai specifikációnak:

A kapcsolódó aláírás-konténer alapprofilja	ETSI TS 103 174 v.2.2.1 (1)

(1) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

Az XML, CMS és PDF formátumú, fokozott biztonságú elektronikus bélyegzőkre és a kapcsolódó bélyegzőkonténerre vonatkozó technikai specifikációk jegyzéke

A határozat 3. cikkében említett fokozott biztonságú elektronikus bélyegzőknek meg kell felelniük az alábbi ETSI technikai specifikációk egyikének, kivéve azok 9. pontját:

XAdES alapprofil	ETSI TS 103 171 v.2.1.1.
CAdES alapprofil	ETSI TS 103 173 v.2.2.1.
PAdES alapprofil	ETSI TS 103 172 v.2.2.2.

A határozat 3. cikkében említett kapcsolódó bélyegzőkonténernek meg kell felelnie az alábbi ETSI technikai specifikációnak:

A kapcsolódó bélyegzőkonténer alapprofilja	ETSI TS 103 174 v.2.2.1.