

## A Kormány

...../2018. (....) Korm. rendelete

### az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről

A Kormány az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 17. § (1a) bekezdés *a)*, *d-f)* pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

#### *1. Hatály, joghatóság*

1. § E rendelet rendelkezéseit kell alkalmazni:

- a)* az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) 2. § *j)* pontja szerinti bejelentés-köteles szolgáltatást nyújtó szolgáltatókra (a továbbiakban: bejelentés-köteles szolgáltató), akik a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény alapján nem tartoznak a mikro- és kisvállalkozások körébe; valamint
- b)* az Ekertv. 2. § *l)* pontja szerinti közvetítő szolgáltatókra (a továbbiakban: közvetítő szolgáltató) a rendelet által meghatározott esetben.

#### *2. A hatóság hatásköre és feladatai*

2. § (1) A Kormány az Ekertv. 6/B. § (3) bekezdése szerinti hatóságként (a továbbiakban: hatóság) a Nemzetbiztonsági Szakszolgálatot jelöli ki. A hatósági jogköröket a Nemzetbiztonsági Szakszolgálat szervezetében működő Nemzeti Kibervédelmi Intézet gyakorolja.

(2) A hatóság a biztonsági események megelőzése, kivizsgálása, felszámolása és terjedésének korlátozása érdekében

*a)* regisztráció alapján nyilvántartást vezet;

*b)* kapcsolatot tart

*ba)* a bejelentés-köteles szolgáltatást nyújtókkal és a közvetítő szolgáltatókkal,

*bb)* a bűnüldöző hatóságokkal,

*bc)* az egyedüli kapcsolattartó ponttal,

*bd)* más tagállamok illetékes ágazati hatóságaival,

*be)* a Nemzeti Adatvédelmi és Információszabadság Hatósággal,

*bf)* az Európai Unióban nem letelepedett, Magyarországon belül szolgáltatásait kínáló bejelentés-köteles szolgáltatást nyújtók által kinevezett képviselővel;

*c)* monitorozza a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-ai (EU) 2016/1148 európai parlamenti és a tanácsi irányelv alkalmazását;

*f)* szükség szerint kötelezi a szolgáltatást nyújtókat arra, hogy

*fa)* bocsássák rendelkezésre az elektronikus információs rendszereik biztonságának megállapításához szükséges adatokat, beleértve a biztonsági szabályzataikra vonatkozóakat is,

*fb)* gondoskodjanak megfelelő biztonsági szint biztosításáról, biztonsági esemény megelőzéséről, bejelentéséről, kezeléséről, továbbá a tapasztalt hiányosságok megszüntetéséről;

*g)* a nyilvánosságot szükség szerint tájékoztatja az egyes biztonsági eseményekről;

*h)* szükség szerint kötelezi a bejelentés-köteles szolgáltatást nyújtót a nyilvánosság tájékoztatására;

*i)* hatósági ellenőrzést végez a bejelentés-köteles szolgáltatást nyújtók kötelezettségeinek teljesítése céljából

*j)* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 19. § (1) bekezdése szerinti eseménykezelő központ (a továbbiakban: eseménykezelő központ) megkeresésére intézkedik a közvetítő szolgáltatókkal szemben.

(3) Ha egy bejelentés-köteles szolgáltató központi ügyvezetésének helye vagy képviselője az egyik tagállamban van, míg az elektronikus információs rendszerei egy vagy több másik tagállamban találhatóak, a központi ügyvezetés helye vagy a képviselő helye szerinti tagállam illetékes hatóságának és az említett másik tagállamok illetékes hatóságainak szükség szerint együtt kell működniük és segíteniük kell egymást. Ez a segítségnyújtás és együttműködés magában foglalhat az érintett illetékes hatóságok közötti információcserét, valamint a 8. § szerinti felügyeleti intézkedések foganatosítására irányuló megkereséseket is.

3. § (1) A hatóság a 2. § (2) bekezdés *a)* pontja szerinti nyilvántartásban kezeli a bejelentés-köteles szolgáltatást nyújtó

*a)* nevét,

*b)* székhelyét,

*c)* cégjegyzékszámát,

*d)* elektronikus kapcsolattartási adatait, valamint

*e)* az általa nyújtott bejelentés-köteles szolgáltatás típusát.

(2) A bejelentés-köteles szolgáltatást nyújtók adatait a hatósági nyilvántartásból törölni kell a gazdasági társaság - tevékenységének megszűnéséről a hatóság részére benyújtott - bejelentése alapján, a bejelentést követő nyolc napon belül.

(3) A hatóság eljárásában a kérelem kormányablaknál való előterjesztése kizárt, valamint az eljárásban kétszeri hiánypótlásra való felszólításnak van helye.

(4) A hatóság intézkedik –, amennyiben bizonyítékokat tárnak elé arra vonatkozóan, hogy valamely bejelentés-köteles szolgáltató nem teljesíti a jogszabályban meghatározott információbiztonsági követelményeket. Ilyen bizonyítékot olyan másik tagállam illetékes hatósága is benyújthat, ahol sor kerül az adott szolgáltatás nyújtására.

(5) A hatóság a hatósági eljárással összefüggésben, további intézkedés keretében

*a)* szükség esetén tájékoztatja az eseménykezelő központokat, egyéb érintett szervezeteket,

*b)* alapvető szolgáltatásokat nyújtó szereplő érintettsége esetén tájékoztatja a kijelölt hatóságot,

*c)* más megelőzési célú intézkedést hoz,

*d)* más hatóság hatáskörébe tartozó eljárást kezdeményez.

(6) A hatóság az eljárása során, feladatai ellátása érdekében - az intézkedéssel érintett bejelentés-köteles szolgáltatást nyújtó működésének és üzemvitelének lehető legkisebb mértékű zavarása mellett - helyszíni ellenőrzés keretében jogosult önállóan, vagy más hatósággal együtt

*a)* az érintett bejelentés-köteles szolgáltatást nyújtó információtechnológiai tevékenységével összefüggő helyiségeibe belépni,

*b)* az érintett bejelentés-köteles szolgáltatást nyújtó számára adatkezelést biztosító, adatfeldolgozást végző, vagy információtechnológiai szempontból érintett helyszínein ellenőrzést tartani, és ennek során bármely, az elektronikus információbiztonsággal

kapcsolatos okiratot, dokumentumot, szerződést, aktív vagy passzív eszközt, információs rendszert, biztonsági intézkedést megismerni, ellenőrizni, az elektronikus információbiztonsággal kapcsolatos elektronikus vagy papíralapú okiratokról, dokumentumokról, szerződésekről, adatbázisokról másolatot készíteni, valamint

c) információtechnológiai műszaki vizsgálatokat végezni, szükség esetén az információtechnológiai rendszerhez egyedileg biztosított belépési jogosultsággal.

(7) A hatóság jogosult helyszíni ellenőrzés keretében vagy a szükséges dokumentumok bekérése útján ellenőrizni a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról szóló, 2018. január 30-i 2018/151/EU bizottsági végrehajtási rendeletben (a továbbiakban: 2018/151/EU bizottsági végrehajtási rendelet) foglalt biztonsági elemek bejelentés-köteles szolgáltató általi teljesítését.

(8) A helyszíni ellenőrzés elrendeléséről az érintett bejelentés-köteles szolgáltatás nyújtó vezetőjét előzetesen írásban, illetve elektronikus úton a helyszíni ellenőrzés megkezdése előtt tíz nappal értesíteni kell.

(9) Az ellenőrzésről az előzetes értesítés mellőzhető, ha

a) súlyos fenyegetettség áll fenn,

b) súlyos biztonsági esemény történt,

c) az a) vagy b) pont szerinti körülmény bekövetkezése valószínűsíthető, vagy

d) az érintett bejelentés-köteles szolgáltatást nyújtó a rendelkezésre álló adatok alapján a helyszíni ellenőrzés eredményes lefolytatását feltehetően megghiúsítaná.

(10) A helyszíni ellenőrzéssel érintett bejelentés-köteles szolgáltatást nyújtó, illetve egyéb érintett közreműködő köteles a hatósággal együttműködni.

(11) A hatóság eljárása során független, képesített ellenőrt igénybe venni, és az általa végzett ellenőrzés eredményét figyelembe venni, valamint a hatóság eljárása során elfogadja az elektronikus információs rendszerek biztonságának szempontjából releváns európai vagy nemzetközileg elfogadott szabványok és előírások szerinti tanúsítványok, akkreditációk alkalmazását.

### *3. A bejelentés-köteles szolgáltatást nyújtók elektronikus és információs rendszereinek biztonságára vonatkozó alapvető követelmények*

4. § (1) A bejelentés-köteles szolgáltatást nyújtó nyújtók elektronikus és információs rendszereinek biztonságára hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról szóló, 2018. január 30-i (EU) 2018/151 bizottsági végrehajtási rendelet az irányadó.

(2) Az (1) meghatározott feladatokat a vonatkozó egyezmények, szabványok, ágazati ajánlások figyelembevételével kell végrehajtani.

(3) A bejelentés-köteles szolgáltatók gondoskodnak azon megfelelő dokumentumok rendelkezésre állásáról, amelyek lehetővé teszik a szolgáltatók rendszerei és létesítményei biztonsága érdekében alkalmazott biztonsági elemek megfelelőségének illetékes hatóság általi ellenőrzését.

5. § (1) A bejelentés-köteles szolgáltatást nyújtó elektronikus úton regisztrál a hatóság honlapján közzétett formában a 2. § (3) bekezdésben meghatározott adatok megadásával.
- (2) Azon bejelentés-köteles szolgáltatást nyújtó, amely e rendelet hatálybalépését követően kerül a rendelet hatálya alá, a változást követő 90 napon belül köteles a 2. § (3) bekezdésben meghatározott adatokat az (1) bekezdésben megjelölt formában benyújtani a hatóságnak.
- (3) A bejelentés-köteles szolgáltatást nyújtó a 2. § (3) bekezdésben meghatározott adatokban bekövetkezett változásokról, továbbá a megszűnéséről 8 napon belül tájékoztatja a hatóságot.

#### *4. A jelentős biztonsági eseményekkel és azok bejelentésével összefüggő szabályok*

6. § (1) A bejelentés-köteles szolgáltatást nyújtó haladéktalanul bejelenti az eseménykezelő központ részére az elektronikus információs rendszerein bekövetkezett azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Európai Unión belül kínált bejelentés-köteles szolgáltatás nyújtására.
- (2) A biztonsági események hatása jelentőségének megállapításakor figyelembe kell venni a 2018/151/EU bizottsági végrehajtási rendeletben meghatározott paramétereket.
- (3) A bejelentés-köteles szolgáltatást nyújtó haladéktalanul bejelenti a Központ részére az elektronikus információs rendszerein bekövetkezett azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Európai Unión belül kínált bejelentés-köteles szolgáltatás nyújtására.
- (4) A biztonsági esemény hatása jelentőségének meghatározása érdekében a bejelentés-köteles szolgáltatást nyújtó szolgáltató tájékoztatásának az alábbi adatokat is tartalmaznia kell:
- a) a biztonsági esemény által érintett felhasználók számát, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását,
  - b) a biztonsági esemény időtartamát,
  - c) a biztonsági esemény által érintett terület földrajzi kiterjedését,
  - d) a szolgáltatás működésében támadt zavar mértékét,
  - e) a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértékét.
- (5) A biztonsági esemény bejelentésére vonatkozó kötelezettség csak abban az esetben áll fenn, ha a bejelentés-köteles szolgáltató számára elérhetők azok az információk, amelyek alapján a (2) bekezdésben említett paraméterek figyelembevételével ki tudja értékelni a biztonsági esemény hatását.
- (6) A biztonsági események hatása jelentőségének megállapításakor figyelembe kell venni a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról szóló, 2018. január 30-i 2018/151/EU bizottsági végrehajtási rendeletben meghatározott paramétereket.
- (7) Az eseménykezelő központ a biztonsági esemény műszaki vizsgálatát követően hatósági eljárás megindítása és lefolytatása céljából a rendelkezésre álló információkat összefoglaló jelentéssel átadja a hatáskörrel és illetékességgel rendelkező hatóság részére.
- (8) A hatóság az eseménykezelő központ összefoglaló jelentése alapján hivatalból indítható hatósági eljárása keretében
- a) vizsgálja a bejelentés-köteles szolgáltatást nyújtó által megtett megelőző és eseményt kezelő tevékenységet;
  - b) vizsgálja az 5. § és 6. §-ban meghatározott követelmények teljesülését;
  - c) vizsgálja a bejelentés-köteles szolgáltatást nyújtó kockázatelemzésének és biztonsági intézkedéseinek megfelelőségét;

- d) a vizsgálathoz a (7) bekezdés szerinti cselekményeket jogosult elvégezni;
- e) a vizsgálat eredményeként hatósági döntést hoz, amelynek tartalma legalább:
  - ea) a biztonsági esemény bekövetkezés tényének megállapítása,
  - eb) az elhárításra javasolt intézkedések,
  - ec) a további károkozások megelőzése érdekében javasolt intézkedések;
- f) az eseménykezelő központtal történt előzetes egyeztetést követően tájékoztathatja a nyilvánosságot vagy kötelezheti a bejelentés-köteles szolgáltatást nyújtót a nyilvánosság tájékoztatására, amennyiben erre egy adott biztonsági esemény megelőzéséhez vagy egy már folyamatban lévő biztonsági esemény kezeléséhez szükség van, vagy ha egy biztonsági esemény nyilvánosságra hozatala egyéb módon közérdeket szolgál.

### *5. Jogkövetkezmények alkalmazása*

7. § (1) A hatóság - határidő kitűzése mellett - felhívja az érintett bejelentés-köteles szolgáltatást nyújtó vezetőjét

- a) az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a biztonsági követelmény megsértésének megszüntetésére,
- b) a jogszabályban meghatározott kötelezettség teljesítésére,
- c) az elvárt intézkedés megtételére.

(2) A hatóság azonnali intézkedések megtételére kötelezi az érintett bejelentés-köteles szolgáltatást nyújtót, ha az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelmény súlyos biztonsági esemény bekövetkeztével fenyeget. Ezzel összefüggésben fegyelmi felelősség megállapítására tehet javaslatot a munkáltatói jogkör gyakorlója felé.

(3) A hatóság az Ekertv. 6/C. §-a alapján az 1. mellékletben megjelölt szabálytalanság esetén az ott rögzített mértékben bírságot szabhat ki.

8. § Ha a közvetítő szolgáltató nem teljesíti a külön Korm. rendeletben meghatározott együttműködési kötelezettségét, a hatóság az eseménykezelő központ értesítése alapján – megfelelő határidő tűzése mellett – felszólítja az érintett szervezetet a jogszabálykövető magatartás folytatására, illetve a határidő eredménytelen eltelte után bírságot szabhat ki.

9. § (1) A kiszabható bírság ötvenezer forinttól ötmillió forintig terjedhet, amelyet a hatóság határozatának véglegessé válását követő nyolc napon belül kell befizetni (a továbbiakban: befizetés) a határozatban megjelölt, a hatóság Magyar Államkincstárnál vezetett számlájára.

(2) A befizetés során az átutalás közlemény rovatában fel kell tüntetni a „digitális bírság” szöveget, a határozat számát és a bírságfizetésre kötelezett nevét.

(3) Több szabálytalanság együttes fennállása esetén a bírság mértéke az egyes szabálytalanságokért kiszabható bírságok összege, amely nem haladhatja meg az ötmillió forintos felső határt.

10. § (1) A bírság megfizetése nem mentesít a büntetőjogi, illetve a polgári jogi felelősség, valamint a bírság kiszabására okot adó szabálytalanság megszüntetésének kötelezettsége alól.

(2) A bírság ugyanazon tényállás mellett – az azonnal megszüntethető szabálytalanságok kivételével – a bírságot kiszabó végleges határozat közlését követő két hónap elteltével szabható ki ismételten.

### *6. A hatósági eljárás során igénybe vehető független szakértőkre vonatkozó rendelkezések*

11. § (1) A hatóság naprakész szakértői névjegyzéket vezet az eljárása során igénybe vehető szakértőkről, valamint az elfogadott hazai és nemzetközi sérülékenység-vizsgálati képzést nyújtó intézményekről.

(2) A névjegyzékbe való bekerüléshez a hatóság évente pályázatot hirdet.

- (3) A pályázati kiírás szakmai előkészítését az eseménykezelő központ végzi, az Ibtv. 19. § (2)-(3) bekezdései szerinti eseménykezelő központok egyetértésével.
- (4) A benyújtásra kerülő pályázatokat bíráló bizottság elnöke az eseménykezelő központ, tagjai a hatóság, az Ibtv. 19. § (2)-(3) bekezdései szerinti eseménykezelő központok és az Alkotmányvédelmi Hivatal által delegált szakértők.
- (5) A szakértői névjegyzékbe felvételt nyert pályázók a hatóság által kiadott szakértői tanúsítványt kapnak, amely három évig érvényes.
- (6) Az (1) bekezdés szerinti jegyzéket a hatóság a honlapján közzéteszi.

## *7. Záró rendelkezések*

12. § Ez a rendelet 2019. január 1-én lép hatályba.

13. § Ez a rendelet

*a)* a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-ai (EU) 2016/1148 európai parlamenti és tanácsi irányelvnek,

*b)* a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról szóló, 2018. január 30-i 2018/151/EU bizottsági végrehajtási rendeletnek való megfelelést szolgálja.

14. § Hatályát veszti a bejelentés-köteles szolgáltatást nyújtókról szóló 410/2017. (XII. 15.) Korm. rendelet.

*1. melléklet a .../2018. (... ..) Korm. rendelethez*

	A	B	C
1.	A jogszabálysértés megnevezése	A bírság legkisebb mértéke (Ft)	A bírság legnagyobb mértéke (Ft)
2.	regisztráció elmulasztása	50 000	100 000
3.	adatváltozás bejelentésének elmulasztása	50 000	500 000
4.	kockázatelemzés készítésének elmulasztása	200 000	500 000
5.	kockázatokkal arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása	300 000	5 000 000
6.	kockázatelemzés és a szükséges biztonsági intézkedések biztonsági eseményt követő haladéktalan, egyéb esetben évente dokumentált felülvizsgálatának elmulasztása, a felülvizsgálat során feltárt hiányosságok alapján a szükséges módosítások végrehajtásának elmulasztása	200 000	2 000 000
7.	biztonsági esemény bejelentésének elmulasztása	300 000	5 000 000
8.	hatóság végleges, végrehajtandó határozatában foglalt kötelezésének nem teljesítése	400 000	5 000 000

## A Kormány

...../2018. (....) Korm. rendelete

### **Az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól**

A Kormány az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés *e*), *j*) és *k*) pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

#### *1. Értelmező rendelkezések*

1. § E rendelet alkalmazásában

1. *adminisztrátori jogosultsággal rendelkező informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy rendszergazdai jogosultsággal rendelkezik, és az eljárás célja, hogy megfelelőségi listák alapján az érintett szervezet teljes informatikai rendszerének az állapota ellenőrzésre kerüljön;
2. *alapvető szolgáltatást nyújtó szolgáltató*: a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.) alapján alapvető szolgáltatást nyújtóként azonosított szolgáltató;
3. *automatizált vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során az érintett szervezet informatikai rendszerének a sérülékenységei célszoftverek segítségével kerülnek feltérképezésre;
4. *bejelentés-köteles szolgáltatást nyújtó*: az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) 2. § j) pontja szerinti szolgáltatást nyújtó szolgáltató;
5. *belső informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során az érintett szervezet informatikai rendszerének sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik;
6. *biztonsági esemény-kezelési megbízott*: az érintett szervezet vezetője által a biztonsági események kivizsgálásával az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 11. § (6) bekezdése szerint megbízott személy;
7. *célszoftverek*: a biztonsági vizsgálati eljárás során a sérülékenységvizsgálat egyes fázisainak végrehajtására kifejlesztett szoftverek;
8. *CSIRT-ek hálózata*: a tagállami számítógép-biztonsági eseményekre reagáló szervezetek a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-ai (EU) 2016/1148 európai parlamenti és tanácsi irányelv (a továbbiakban: Irányelv) által létrehozott hálózata;
9. *érintett szervezet*: a biztonsági vizsgálatlal vagy sérülékenységvizsgálattal érintett, elektronikus információs rendszert üzemeltető szervezet;
10. *kézi informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során az érintett szervezet informatikai rendszerének sérülékenységei a vizsgálatot

végző személy által egyedileg, manuálisan összeállított lekérdezések alkalmazásával kerülnek feltérképezésre;

11. *közvetítő szolgáltató*: az Ekertv. 2. § 1) pontja szerinti szolgáltató;
12. *külső informatikai biztonsági vizsgálat*: az informatikai rendszer internet felőli, külső sérülékenységvizsgálata, amelynek során az interneten fellelhető, nyilvános adatbázisokban való szabad keresésre, célzott információgyűjtésre, valamint az elérhető számítógépek szolgáltatásainak, sebezhetőségének feltérképezésére kerül sor;
13. *regisztrált felhasználói jogosultság nélküli informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy semmilyen előzetes információval nem rendelkezik az érintett szervezet informatikai rendszeréről, és nincs felhasználói jogosultsága a rendszerhez;
14. *regisztrált felhasználói jogosultsággal rendelkező informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy a számára külön létrehozott felhasználói jogosultsággal végzi a vizsgálatot;
15. *pszichológiai befolyásolás*: olyan kibertámadási forma, technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését;
16. *titkosítási eljárás*: olyan eljárás, amely az adat megismerhetőségét azáltal korlátozza, hogy az adat egy algoritmus segítségével átalakításra kerül olyan jelsorozattá, ami olvashatatlan azon személy számára, aki nem rendelkezik a visszaalakításhoz szükséges egyedi jelsorozatból álló kulccsal;
17. *titkosítási kulcs*: titkosítási eljárás során alkalmazott olyan jelsorozat, amelynek ismeretében a titkosított állomány megismerhető;
18. *webes vizsgálat*: olyan biztonsági vizsgálati eljárás, amely során automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei;
19. *vezeték nélküli hálózat informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik.

## 2. A Központ feladat- és hatásköre

2. § (1) A Kormány az Ibtv. 19. § (1) bekezdése, valamint az Ekertv. 6/B. § (1) bekezdése alapján eseménykezelő központként (a továbbiakban: Központ) a Nemzetbiztonsági Szakszolgálatot jelöli ki.

(2) A Központ jelen rendeletben meghatározott jogköreit a Nemzetbiztonsági Szakszolgálat szervezetében működő Nemzeti Kibervédelmi Intézet gyakorolja.

3. § (1) A Központ támogatja

a) az Ibtv. 19. § (1) bekezdés b) pontja szerinti infrastruktúrát, illetve elektronikus információs rendszert működtető szerveket (a továbbiakban: állami és önkormányzati szervek),

b) a bejelentés-köteles szolgáltatókat és a közvetítő szolgáltatókat,

c) az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetőket,

d) a központosított informatikai és elektronikus hírközlési szolgáltatót

azok elektronikus információs rendszereiben bekövetkezett biztonsági események kezelése tekintetében.

(2) A Központ a biztonsági események és fenyegetések kezelése céljából együttműködik

- a) az elektronikus információs rendszerek felügyeletére kijelölt hatóságokkal,
- b) az Ibtv. 19. § (2)-(3) bekezdése szerint kijelölt eseménykezelő központokkal (a továbbiakban együtt: eseménykezelő központok),
- c) a bűnüldöző hatóságokkal,
- d) a Nemzeti Média- és Hírközlési Hatósággal és az általa működtetett Országos Informatikai és Hírközlési Főigazgatósággal,
- e) az elektronikus hírközlési szolgáltatókkal, a központosított informatikai és elektronikus hírközlési szolgáltatóval,
- i) az Lrtv. szerinti ágazati szereplőkkel,
- j) az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet szerinti egyedüli kapcsolattartó ponttal (a továbbiakban: egyedüli kapcsolattartó pont), valamint
- k) a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

(3) A Központ - az érintett eseménykezelő központ kezdeményezésére - segítséget kérhet az Európai Hálózat- és Információbiztonsági Ügynökségtől az eseménykezelő központok továbbfejlesztéséhez.

(4) A Központ a hatáskörébe tartozó elektronikus információs rendszerek tekintetében részt vesz a CSIRT-ek hálózatának tevékenységében.

(5) A Központ a biztonsági eseményre vagy fenyegetésre utaló tevékenységeket kivizsgálja és szükség esetén figyelmeztetést ad ki a központosított informatikai és elektronikus hírközlési szolgáltató, a felhasználók, az eseménykezelő központok, a hatóságok és az egyedüli kapcsolattartó pont felé.

(6) A Központ – a biztonsági eseményben érintett szervvel folytatott egyeztetést követően – szükség szerint tájékoztathatja a nyilvánosságot az egyes biztonsági eseményekről, illetve szükség szerint kötelezi az (1) bekezdés szerinti szerveket a nyilvánosság tájékoztatására amennyiben erre egy adott biztonsági esemény megelőzéséhez vagy egy már folyamatban lévő biztonsági esemény kezeléséhez szükség van.

(7) A Központ tájékoztatja az egyedüli kapcsolattartó pontot a biztonsági események kezelésére vonatkozó, jogszabályban nem részletezett eljárásrendjéről.

(8) A Központ ellátja az alábbi feladatokat:

- a) a biztonsági események nemzeti szintű monitoringja;
- b) a kockázatokkal és biztonsági eseményekkel kapcsolatos tájékoztatás, korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek számára;
- c) reagálás a biztonsági eseményekre;
- d) dinamikus kockázat- és eseményelemzéseket, valamint a biztonsági eseményekkel kapcsolatos helyzetképet készít;
- h) sérülékenységvizsgálat lefolytatása.

(9) A Központ meghatározza a biztonsági események és kockázatok kezelésére vonatkozó eljárásokat, valamint a biztonsági események, kockázatok és információk osztályozására szolgáló eljárásokat és szabályokat. Ennek során a Központ együttműködik az (1) bekezdésben meghatározott szervezetekkel.

4. § A Központ a biztonsági esemény-kezelési feladatkörében felelős

- a) a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítéséért, valamint
- b) a biztonsági eseményekről nyilvántartás vezetéséért, amely tartalmazza a biztonsági esemény kapcsán megtett intézkedéseket és azok eredményét.

5. § (1) A Központ a biztonsági események megelőzése céljából a 3. § (1) bekezdés szerinti szervezetek elektronikus információs rendszereit érintő fenyegetésekkel összefüggő tájékoztatási és tudatosítási feladatokat a (2)-(4) bekezdésben meghatározottak szerint látja el.

(2) A Központ az elektronikus információs rendszereket veszélyeztető sérülékenységekkel és fenyegető kockázatokkal összefüggésben felelős

- a) az elektronikus információs rendszerek biztonságáért felelős személyek tájékoztatásáért,
- b) a hatóságok és az eseménykezelő központok tájékoztatásáért, valamint
- c) a sérülékenységekről és fenyegetésekről, valamint a javasolt biztonsági intézkedésekről a honlapján rendszeres tájékoztatás nyújtásáért.

(3) A Központ

- a) elemzéseket, jelentéseket készít a magyar és nemzetközi információbiztonsági irányokról,
- b) a hatáskörébe tartozó biztonsági eseményekről negyedévente jelentést tesz a Nemzeti Kiberbiztonsági Koordinációs Tanács részére, valamint
- c) évente jelentést készít a tevékenységéről a Központot irányító miniszter részére.

(4) A Központ

- a) nem kötelező érvényű állásfoglalásokat, ajánlásokat adhat ki,
- b) a biztonsági események kezelésére irányuló tájékoztatót tarthat, részt vehet az információbiztonság tudatosításáért felelős intézmények tudatosítási programjában, szakértői-oktatói tevékenységet végezhet,
- c) kormányzati információtechnológiai, és biztonságiesemény-kezelési együttműködési fórumot működtethet, valamint
- d) részt vesz az infokommunikációs biztonságra vonatkozó stratégiák és szabályozások előkészítésében.

6. § (1) A Kormány az Ibtv. 19. § (2) bekezdése alapján a honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelésére a Katonai Nemzetbiztonsági Szolgálatot jelöli ki. A Katonai Nemzetbiztonsági Szolgálat a biztonsági események és fenyegetések kezelését a szakmai irányítása és koordinálása alatt álló, szakfeladat szerint elkülönülő - a honvédelemért felelős miniszter irányítása, vezetése alatt álló szervnél, szervezetnél működő - eseménykezelő központokkal együtt látja el.

(2) A Kormány az Ibtv. 19. § (3) bekezdése alapján a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelésére az Információs Hivatalt jelöli ki. Az Információs Hivatal e feladat ellátására a szervezeti keretén belül működő eseménykezelő központot működtet.

(3) Az eseménykezelő központok megosztják a Központtal a szolgáltatási, operatív és együttműködési képességeikkel kapcsolatos információkat.

(4) Az eseménykezelő központok a hatáskörükbe tartozó elektronikus információs rendszerek tekintetében,

- a) biztonságiesemény-kezelési feladatkörükben ellátják a Központ 4. §,
- b) tájékoztatási feladatkörükben ellátják a Központ 5. § (2) bekezdés b) pontja, és 5. § (3) bekezdés c) pontja,
- c) tudatosítási feladatkörükben ellátják a Központ 5. § (4) bekezdés a)-c) pontja szerinti feladatait.

#### *1. Az eseménykezelő központok feladat- és hatásköre*

7. § (1) Az eseménykezelő központok a hatáskörükbe tartozó elektronikus információs rendszerek tekintetében

- a) nyilvántartást vezetnek a hatáskörükbe tartozó szervekkel való kapcsolattartáshoz szükséges elérhetőségekről, és

b) az észlelt, valamint a tudomásukra jutott biztonsági eseményekről haladéktalanul tájékoztatják a Központot.

(2) Az eseménykezelő központok a működésük megkezdéséről - működésüknek a tervezett megkezdését megelőzően legalább öt nappal - a Központot tájékoztatják, a kapcsolattartáshoz szükséges adatokat, valamint a kapcsolattartási adatok változását haladéktalanul bejelentik a Központnak.

## 2. A biztonsági események bejelentése

8. § Az Ibtv. 19. § (1) bekezdés b)-c) pontja szerinti szervezetek, valamint a közvetítő szolgáltató kötelesek a Központ részére az elektronikus információs rendszereikben bekövetkezett biztonsági eseményeket haladéktalanul bejelenteni.

9. § (1) Az alapvető szolgáltatást nyújtó szolgáltatók indokolatlan késedelem nélkül bejelentik a Központnak az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket.

(2) A biztonsági esemény hatása jelentőségének meghatározása érdekében az alapvető szolgáltatást nyújtó szolgáltató tájékoztatásának az alábbi adatokat is tartalmaznia kell:

a) az alapvető szolgáltatás zavara által érintett felhasználók száma;

b) a biztonsági esemény időtartama;

c) a biztonsági esemény által érintett terület földrajzi kiterjedése.

(3) Amennyiben egy alapvető szolgáltatásokat nyújtó szolgáltató valamely, a kritikus társadalmi és gazdasági tevékenységek fenntartása szempontjából alapvetőnek tekintett szolgáltatás nyújtását egy harmadik fél bejelentés-köteles szolgáltatóra alapozza, az említett szolgáltatónak be kell jelentenie minden olyan esetet, amikor a bejelentés-köteles szolgáltatót érintő biztonsági esemény jelentős hatást gyakorol az alapvető szolgáltatások folytonosságára.

10. § A bejelentés-köteles szolgáltatást nyújtó, a külön kormányrendeletben meghatározottak szerint haladéktalanul bejelenti a Központ részére az elektronikus információs rendszerein bekövetkezett azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Európai Unión belül kínált bejelentés-köteles szolgáltatás nyújtására.

11. § (1) A biztonsági események bejelentése elsődlegesen elektronikus úton történik, ha azonban az elektronikus információs rendszer oly mértékben sérül, hogy az nem lehetséges, a bejelentés bármely más módon megvalósítható.

(2) A bejelentés tartalmazza legalább

a) az esemény rövid leírását, státuszát,

b) a szolgáltatás működésében támadt zavar mértékét,

c) az esemény kezelésére az üzemeltető által kijelölt kapcsolattartó személy és szervezet elérhetőségeit,

d) a biztonsági esemény hatását meghatározó szempontokat, valamint

e) közvetítő szolgáltató igénybevétele esetén a közvetítő szolgáltató megnevezését, elérhetőségét.

12. § (1) A Központ – a 9. § (1) és a 10. § (1) bekezdés szerinti bejelentések alapján - vizsgálja az alapvető-, valamint a bejelentés-köteles szolgáltatást nyújtók szolgáltatásaira jelentős hatást gyakorló biztonsági események határon átnyúló hatását, és közvetlenül vagy az egyedüli kapcsolattartó pont útján indokolt esetben tájékoztatja a jelentős hatást gyakorló biztonsági eseményekről a többi érintett tagállamot.

(2) A Központnak az (1) bekezdés szerinti tájékoztatás során biztosítani kell a szolgáltatók biztonságát, gondoskodnia kell arról, hogy ne sérüljenek a kereskedelmi érdekei és a bejelentésben foglalt információk bizalmassága.

### *5. Önkéntes bejelentés*

13. § (1) Azok az Lrtv. szerinti ágazati szereplők, akiket nem azonosítottak alapvető szolgáltatásokat nyújtó szolgáltatóként, önkéntes alapon bejelenthetik a Központnak az olyan biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általuk nyújtott szolgáltatások folytonosságára. Ez a rendelkezés nem alkalmazható azon rendszerelemek vonatkozásában, amelyek az Lrtv. alapján európai vagy nemzeti létfontosságúvá kerültek kijelölésre.

(2) A bejelentés-köteles szolgáltatók önkéntes alapon bejelenthetnek minden olyan eseményt, amelyek számukra addig ismeretlen jellemzőkkel bírtak, ideértve különösen a sérülékenységet kihasználó új módszereket, a kihasználásra vonatkozó adatokat sebezhető pontokat vagy fenyegetéseket.

(3) A Központ az önkéntes bejelentésekkel szemben előnyben részesítheti a kötelezően vizsgálendő bejelentések feldolgozását. Az önkéntes bejelentéseket csak akkor kell feldolgozni, ha az nem jelent aránytalan vagy indokolatlan terhet a Központ számára.

(4) Az önkéntes bejelentés eredményeként a bejelentő szervezet számára nem írható elő olyan kötelezettség, amely ne vonatkozott volna rá a bejelentés megtétele nélkül is.

### *6. A biztonsági események kezelésének, műszaki vizsgálatának szabályai*

14. § Az állami és önkormányzati szervek elektronikus információs rendszereit érintő biztonsági események kivizsgálásában első sorban

a) az elektronikus információs rendszer biztonságáért felelős személy,

b) biztonságiesemény-kezelési megbízott, valamint

c) a hatáskörrel rendelkező eseménykezelő központ vehet részt.

15. § (1) A nemzetbiztonsági védelem alá eső szerv vezetője - a 6. § (1)-(3) bekezdésben meghatározott szervek kivételével -

a) az elektronikus információs rendszer biztonságáért felelős személy esetében a feladatra történő kinevezése,

b) a biztonságiesemény-kezelési megbízott esetében a feladatra történő megbízása tervezett hatálybalépését megelőző harminc nappal véleményezés céljából - az érintett személy hozzájárulásával - megküldi a Központ részére a kinevezésben, illetve a megbízásban szereplő személy adatait.

(2) A Központ a feladatra történő kinevezés, illetve a megbízás hatálybalépésének időpontjáig köteles a véleményét a véleménykérő szerv vezetője részére megküldeni.

(3) A biztonságiesemény-kezelési megbízottat az Ibtv.-ben meghatározott elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személynek kell tekinteni.

16. § (1) A bejelentett incidensek kivizsgálása során a biztonsági eseménnyel érintett szervezet köteles együttműködni a Központtal, amely együttműködés kiterjed:

a) a bejelentéssel kapcsolatos információk átadására,

b) a biztonsági eseményben érintettek (támadó/támadott) beazonosításához szükséges műszaki, technikai adatok Központ részére történő átadására,

c) a Központ szakembereinek tájékoztatására az incidens következményei elhárítása érdekében tett intézkedésekről, illetve az incidens vizsgálata során, az infrastruktúrával kapcsolatos beállításokról,

d) hozzáférés biztosítására a Központ szakemberei számára az incidensben érintett infrastruktúrához, valamint

e) a Központ által végzett kockázatelemzés alapján szükségesnek ítélt korai figyelmeztető-, vagy csapdarendszerek, szenzorok telepítésére.

(2) Az együttműködés keretein belül az alapvető szolgáltatást nyújtó szolgáltatók az incidensben érintett infrastruktúrával kapcsolatos, speciális, ágazati sajátosságokat megosztják a Központtal.

(3) A bejelentés-köteles szolgáltatók, valamint az Lrtv. 4. melléklet 26. sora szerinti alapvető szolgáltatást nyújtó szolgáltatók az együttműködés keretein belül az incidensben érintett előfizetőkkel kapcsolatban a Központ kérésére kötelesek szükség szerint tiltásokat bevezetni, illetve (felhasználói, előfizetői) hozzáféréseket korlátozni, felfüggeszteni, vagy megszüntetni.

17. § (1) A biztonsági eseménnyel érintett szervezet – a (2) bekezdés kivételével – a Központ kérésére köteles a biztonsági események kezeléséhez szükséges műszaki, technikai adatokat, információkat összegyűjteni és elektronikus formában átadni vagy egyéb módon hozzáférhetővé tenni.

(2) Ha a biztonsági eseménnyel érintett szervezet – a (3) bekezdés kivételével – bármely okból nem képes az adatok összegyűjtésére, a Központ begyűjtheti az adatokat. A biztonsági eseménnyel érintett szervezet gondoskodik arról, hogy a Központ az adatokhoz hozzáférjen.

(3) Ha a biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtó bármely okból nem képes az (1) bekezdés szerinti adatok összegyűjtésére, az eseménykezelő központ képviselője helyszíni tanácsadás keretein belül, az érintett szervezet szakértőinek bevonásával javaslatot tesz a szükséges adatok összegyűjtésének és biztosításának módjára. A biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtó gondoskodik arról, hogy az eseménykezelő központ az adatokhoz hozzáférjen.

(4) A biztonsági eseményekkel érintett szerv – az (5) bekezdés kivételével – köteles a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a Központ rendelkezésére bocsátani.

(5) A biztonsági eseményekkel érintett bejelentés-köteles szolgáltató köteles a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat tartalmazó, bithú másolatokat a Központ rendelkezésére bocsátani.

(6) A Központ – a (7) bekezdés kivételével – a biztonsági eseménnyel érintett szervezettel együttműködve kidolgozza a biztonsági esemény felszámolásához szükséges intézkedéseket, amelyeket a biztonsági eseménnyel érintett szervezet köteles végrehajtani.

(7) A biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtó a biztonsági esemény felszámolásához szükséges intézkedéseket kidolgozza és haladéktalanul végrehajtja. A Központ támogatja a biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtót a biztonsági esemény felszámolásához szükséges intézkedések kidolgozásában.

(8) A biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtó az esemény felszámolását követően felülvizsgálja az elektronikus információs rendszerei kockázatelemzésének, kockázatkezelésének teljességét, és végrehajtja a szükséges módosításokat.

(9) A Központ a biztonsági eseményről szigorúan zárt kezelésű technológiai naplót vezet, amely tartalmazza a biztonsági esemény kivizsgálásának támogatása során tett intézkedéseket, és azok eredményét is.

18. § (1) A Központ a hatáskörébe tartozó elektronikus információs rendszert működtető szervektől és az eseménykezelő központoktól kért és kötelezően átadott információk és adatok alapján, az elektronikus információs rendszereket érintő, biztonsági eseményre vagy fenyegetésre utaló jeleket elemezi, kiértékeli, és folyamatos ügyeleti rendszerén keresztül értesíti az elektronikus információs rendszer üzemeltetőjét a biztonsági esemény bekövetkeztének veszélyéről vagy fennállásáról, valamint a javasolt intézkedésekről.

(2) A Központ a központosított informatikai és elektronikus hírközlési szolgáltatótól átvett műszaki adatok és információk folyamatos figyelésével értékelést végezhet, valamint keresheti a hálózatok, illetve szolgáltatások működését érintő biztonsági eseményre vagy fenyegetésre utaló jeleket.

(3) A központosított informatikai és elektronikus hírközlési szolgáltató a Központ által történő biztonsági esemény-kezelés során köteles

a) a biztonsági eseményben érintettek (támadó/támadott) beazonosításához szükséges műszaki, technikai adatok Központ részére történő átadására,

b) az ismert fenyegetések elleni védelmi intézkedések, műszaki, technikai megoldások alkalmazására,

c) a Központ kérésére adatokat szolgáltatni a hálózati forgalomba való beavatkozásra utaló jelek elemzése, kiértékelése céljából, valamint

d) a Központ által meghatározott, biztonsági eseményekkel kapcsolatos feladatokban együttműködni.

19. § (1) A biztonsági események kivizsgálása során az eseménykezelő központ szükség szerint megismerheti a közvetítő szolgáltatók különböző szolgáltatás- vagy üzletmenet folytonosságot biztosító szabályzóit, eljárásrendjeit (különösen üzletfolytonossági tervét, katasztrófa helyreállítási tervét).

(2) A biztonsági esemény által érintett közvetítő szolgáltató az eseménykezelő központtal való együttműködés keretein belül a konkrét biztonsági esemény kezelése érdekében az eseménykezelő központ kérésére a biztonsági eseményben érintettek (támadó/támadott) beazonosításához szükséges adatokat szolgáltat a Központ részére, valamint az incidensben érintett előfizetőkkel kapcsolatban szükség szerint tiltásokat vezet be, (felhasználói, előfizetői) hozzáféréseket korlátoz, függeszt fel, vagy szüntet meg.

(3) Veszélyesnek vagy károsnak ítélt szolgáltatás biztosítása esetén az eseménykezelő központ kötelezheti a közvetítő szolgáltatót adott szolgáltatás tiltására.

(4) A Központ értesítése alapján az Ekertv. 6/B. § (3) bekezdése alapján kijelölt hatóság külön Korm. rendeletben meghatározott mértékű bírságot szabhat ki, ha a közvetítő szolgáltató nem teljesíti együttműködési kötelezettségét.

20. § A biztonsági eseményekkel összefüggő adatok műszaki vizsgálatának célja, hogy a bekövetkezett biztonsági események kivizsgálása révén a Központ

a) feltárja a biztonsági esemény bekövetkeztének okait, körülményeit, az okozott kár mértékét,

b) behatárolja a biztonsági esemény által érintett elektronikus információs rendszerek, rendszerelemek körét,

c) javaslatot tegyen a biztonsági esemény által okozott kár elhárítására, és

d) a bekövetkezett biztonsági eseményből levonható tanulságokról tájékoztassa a biztonsági eseménnyel érintett más szerveket és a hatóságot annak érdekében, hogy a jövőben a biztonsági esemény bekövetkezése megelőzhető legyen.

21. § A bejelentési, tájékoztatósi, illetve együttműködési kötelezettségnek eleget nem tevő szervezetet a Központ jelenti az adott elektronikus információs rendszer felügyeletét ellátó hatóságnak.

### 7. Sérülékenységvizsgálat

22. § (1) A nemzetbiztonsági védelem alá eső szervek elektronikus információs rendszerei, az Ibtv. 2. § (1) bekezdése szerinti állami és önkormányzati szervek európai létfontosságú rendszerelémmé vagy nemzeti létfontosságú rendszerelémmé törvény alapján kijelölt rendszerlemeinek elektronikus információs rendszerei, valamint a zárt célú elektronikus információs rendszerek sérülékenységvizsgálatát - a (2) és (3) bekezdésben meghatározott kivétellel - a Központ végzi. A Központ jogosult továbbá az Ibtv. 18. § (3) bekezdése szerinti állami szervként a sérülékenységvizsgálat lefolytatására.

(2) A polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei sérülékenységvizsgálatát a 6. § (2) bekezdése szerinti eseménykezelő központ végzi.

(3) A honvédelmi célú elektronikus információs rendszerek sérülékenységvizsgálatát a 6. § (1) bekezdése szerinti eseménykezelő központ végzi.

(4) Az Ibtv. 18. § (3) bekezdés *b)* pontja szerinti gazdasági társaság (a továbbiakban: gazdasági társaság) abban az esetben végezhet sérülékenységvizsgálatot, ha

*a)* a gazdasági társaság nevében és alkalmazásában eljárva a sérülékenységvizsgálatban részt vevő személy az Ibtv.-ben meghatározott feltételeken túl rendelkezik a sérülékenységvizsgálat lefolytatásához szükséges ismeretek meglétét igazoló végzettséggel, és ezen a szakterületen legalább 2 év szakmai tapasztalattal, valamint

*b)* a gazdasági társaság bejegyzésre került a sérülékenységvizsgálat lefolytatására jogosult gazdasági társaságok nyilvántartásába.

(5) A sérülékenységvizsgálat lefolytatására jogosult gazdasági társaságokról az Alkotmányvédelmi Hivatal - személyes adatot nem tartalmazó - nyilvántartást vezet. A nyilvántartás tartalmazza a gazdasági társaság adatait, a sérülékenységvizsgálatban részt vevő személyek számát és a sérülékenységvizsgálat lefolytatásához szükséges ismereteket igazoló végzettség megnevezését és megszerzési idejét.

(6) Az (5) bekezdés szerinti adatok tekintetében az Alkotmányvédelmi Hivatal egyéni, írásbeli kérelem alapján, annak beérkezésétől számított tizenöt napon belül nyújt tájékoztatást azon elektronikus információs rendszereket üzemeltető szervezet részére, amelyek az Ibtv. 18. § (2) bekezdése alapján jogosultak sérülékenységvizsgálatot kezdeményezni.

(7) A nyilvántartásba való felvételt a gazdasági társaság kezdeményezi az Alkotmányvédelmi Hivatal felé, a (4) bekezdésben meghatározott feltételek meglétét igazoló okiratok benyújtásával. A (4) bekezdésben meghatározott feltételek szakmai megfelelése tekintetében a Központ nyilatkozata irányadó.

(8) Az Alkotmányvédelmi Hivatal elutasítja a nyilvántartásba történő felvételi kérelmet, ha

*a)* a gazdasági társaság nem rendelkezik az Ibtv. 18. § (3) bekezdés *b)* pontjában megkövetelt telephely biztonsági tanúsítvánnyal,

*b)* a Központ nyilatkozata alapján a sérülékenységvizsgálat lefolytatásához szükséges ismeretek meglétét igazoló végzettség, és ezen a szakterületen legalább 2 év szakmai tapasztalat nem áll fenn, vagy

*c)* a gazdasági társaság által közölt adatok a valóságnak nem felelnek meg.

(9) A sérülékenységvizsgálat lefolytatására jogosult gazdasági társaság az alkalmassági feltételeket érintő változásokról, valamint a sérülékenységvizsgálatban részt vevő személyeket érintő változásokról a változást követő nyolc napon belül értesíti az Alkotmányvédelmi Hivatalt.

(10) Az Alkotmányvédelmi Hivatal jogosult az alkalmassági feltételek meglétét, valamint a nyilvántartásban szereplő adatok valódiságát ellenőrizni. Az értesítési kötelezettség elmulasztása esetén, valamint az alkalmassági feltételek meglétének hiánya esetén az Alkotmányvédelmi Hivatal a gazdasági társaságot a nyilvántartásából törli.

(11) Az (5) bekezdés szerint vezetett nyilvántartásba felvételre került gazdasági társaságnak a felvételt követő minden második évben, az Alkotmányvédelmi Hivatal által a felvételtől kiállított tanúsítványban feltüntetett hónapnak megfelelő hónap utolsó napjáig a (4) és (7) bekezdés szerinti okiratokat – a biztonsági vezető útján – ismételten meg kell küldenie az AH részére.

(12) Az Alkotmányvédelmi Hivatal a megküldött dokumentumok alapján ismételten ellenőrzi, hogy teljesülnek-e a (4) bekezdésben meghatározott feltételek.

(13) Ha (11) bekezdésben meghatározott adatszolgáltatási kötelezettségének a gazdasági társaság nem tesz eleget, az Alkotmányvédelmi Hivatal törli a nyilvántartásból.

23. § (1) A sérülékenységvizsgálat célja az esetleges biztonsági események bekövetkeztét megelőzően az érintett szervezet elektronikus információs rendszere, rendszerelemei gyenge pontjainak feltárása, valamint a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása az elektronikus információs rendszerek, rendszerelemek védelmének és biztonságának megerősítése érdekében.

(2) A sérülékenységvizsgálat tárgya az adatok, információk kezelésére használt elektronikus információs rendszerek, rendszerelemek, eszközök, eljárások és kapcsolódó folyamatok vizsgálata, valamint az ezeket kezelő személyek általános informatikai felkészültségének, és az érintett szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata.

24. § (1) A sérülékenységvizsgálat során a sérülékenységvizsgálati eljárását megalapozó dokumentációban meghatározottak szerint az alábbi vizsgálatok elvégzésére kerül sor:

a) külső informatikai biztonsági vizsgálat,

b) webes vizsgálat,

c) automatizált vizsgálat,

d) pszichológiai befolyásolás,

e) belső informatikai biztonsági vizsgálat, illetve

f) vezeték nélküli hálózat informatikai biztonsági vizsgálata.

(2) A sérülékenységvizsgálat az (1) bekezdésben meghatározott irányultságok tekintetében három típusú jogosultsági fázist tartalmazhat:

a) regisztrált felhasználói jogosultság nélküli vizsgálat,

b) regisztrált felhasználói jogosultsággal rendelkező vizsgálat és

c) adminisztrátori jogosultsággal rendelkező vizsgálat.

(3) A sérülékenységvizsgálat határideje a hatóság határozatának keltétől, illetve az előzetesen egyeztetett kezdési időponttól számítva az (1) bekezdésben meghatározott vizsgálatok szerint:

a) külső informatikai biztonsági vizsgálat esetén harminc nap,

b) webes vizsgálat esetén hetvenöt nap,

c) belső informatikai biztonsági vizsgálat esetén kilencven nap,

d) vezeték nélküli hálózat informatikai biztonsági vizsgálat esetén harminc nap.

25. § (1) A sérülékenységvizsgálat előkészítése során a sérülékenységvizsgálatot végző szerv sérülékenységvizsgálati dokumentációt készít. A sérülékenységvizsgálati dokumentációban rögzíti a vizsgálati feladatokat, célokat, a technikai és személyi feltételeket, a módszertant, az egyeztetések, a sérülékenységvizsgálat várható befejezésének dátumát.

(2) Ha a sérülékenységvizsgálatot a hatóság rendeli el, akkor a sérülékenységvizsgálati dokumentációban a határozatban rögzített vizsgálati feladatokat kell feltüntetni. A sérülékenységvizsgálat egyedi kezdeményezése esetén a vizsgálati feladatokra a kezdeményező javaslatot tehet, amelyről a sérülékenységvizsgálatot végző szerv dönt.

(3) A sérülékenységvizsgálati dokumentációt a sérülékenységvizsgálatot végző szerv megküldi az érintett szervezet részére. Az érintett szervezet a sérülékenységvizsgálati dokumentáció tartalmára a kézhezvételtől számított nyolc napon belül észrevételt tehet. Az észrevétel nem érintheti a hatóság által elrendelt vizsgálatokat. Az észrevételekről a sérülékenységvizsgálatot végző szerv dönt.

26. § (1) A sérülékenységvizsgálatot végző szerv a sérülékenységvizsgálat során kellő gondossággal eljárva, törekedni köteles a vizsgált elektronikus információs rendszer által nyújtott szolgáltatások szükségesnél nem nagyobb mértékű korlátozására, a sérülékenységvizsgálatnak a szolgáltatás szempontjából nem kritikus időszakban történő elvégzésére. A sérülékenységvizsgálatot végző szerv köteles a korlátozás várható mértékéről és időtartalmáról az érintett szervezetet előzetesen tájékoztatni.

(2) Hatósági határozat alapján elrendelt sérülékenységvizsgálat esetén az érintett szervezet köteles a sérülékenységvizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a sérülékenységvizsgálatot végző szerv rendelkezésére bocsátani, valamint túrni a sérülékenységvizsgálatból fakadó, a vizsgált elektronikus információs rendszeren bekövetkezett szolgáltatáscsökkenést.

(3) Egyedi kezdeményezés esetén az érintett szervezet a 25. § (3) bekezdés szerinti észrevételezés során kizárhatja azon vizsgálatokat, amelyek jelentős szolgáltatáscsökkenést eredményeznek.

(4) A sérülékenységvizsgálatot végző szerv a sérülékenységvizsgálatra irányadó határidőt, annak letelte előtt egy alkalommal legfeljebb harminc nappal meghosszabbíthatja, és erről az érintett szervezetet és a hatóságot értesíti.

27. § (1) A Központ saját hatáskörében indított sérülékenységvizsgálat végrehajtása érdekében a 22 § szerinti szervezetek kötelesek bejelenteni a webes szolgáltatások (weboldalak, web-szerverek) elérhetőségére vonatkozó egyedi technikai adatokat, azonosítókat a Központ részére.

(2) A webes szolgáltatások elérhetőségében bekövetkező változás esetén a bejelentést 3 napon belül meg kell tenni.

(3) A Központ tájékoztatja az érintett szervezetet az általa a vizsgálatához használt IP címről, vagy más egyedi technikai azonosítóról, amelyet az érintett szervezet nem tilthat ki a webes szolgáltatás eléréséből.

28. § (1) Az érintett szervezet elektronikus információs rendszere az átlagostól jelentősen eltér, ha

a) az elektronikus információs rendszer

aa) a külső internetes tartományban több mint 20 IP címen elérhető eszközzel,

ab) több mint 10 webes szolgáltatással,

ac) a belső hálózat tekintetében több mint 50 szerverrel,

ad) több mint 500 munkaállomással,

ae) több mint 5 vezeték nélküli hálózattal, vagy

af) több mint 500 fős felhasználói létszámmal

rendelkezik, vagy

b) az érintett szervezet több mint három telephelyen rendelkezik a vizsgálatot érintett elektronikus információs rendszerrel.

(2) Ha az érintett szervezet elektronikus információs rendszere, rendszereleme az átlagostól jelentősen eltér és emiatt egyedi sérülékenységvizsgálati eljárás szükséges, a sérülékenységvizsgálati határidő a 24. § (3) bekezdésben meghatározottakon túl további harminc nappal meghosszabbítható.

29. § (1) A sérülékenységvizsgálat lezárásakor a sérülékenységvizsgálatot végző szerv állásfoglalást készít, és azt nyolc napon belül megküldi az érintett szervezet és a hatóság részére.

(2) Az (1) bekezdés szerinti állásfoglalás tartalmazza:

a) a vizsgálati eredmények leírását, és

b) a rövid-, közép- és hosszú távú intézkedésekre vonatkozó intézkedési javaslatokat.

#### *8. Záró rendelkezések*

30. § Ez a rendelet 2019. január 1-én lép hatályba.

31. § Ez a rendelet

a) a belső piaci szolgáltatásokról szóló, 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelvnek;

b) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i 2016/1148/EU európai parlamenti és tanácsi irányelvnek;

c) a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról szóló, 2018. január 30-i 2018/151/EU bizottsági végrehajtási rendeletnek való megfelelést szolgálja.

32. § E rendelet tervezetének a belső piaci szolgáltatásokról szóló 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelv 15. cikk (7) bekezdése szerinti előzetes bejelentése megtörtént.

33. § Hatályát veszti a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet.

## A Kormány

...../2018. (....) Korm. rendelete

### **egyes belügyi tárgyú és más kapcsolódó törvények módosításáról szóló 2018. évi ... törvénnyel összefüggő Korm. rendeletek módosításáról**

A Kormány a külföldre utazásról szóló 1998. évi XII. törvény 41. § (1) bekezdésében,  
a 2. alcím tekintetében a minősített adat védelméről szóló 2009. évi CLV. törvény 37. § *e*)  
pontjában,  
a 3. alcím tekintetében a minősített adat védelméről szóló 2009. évi CLV. törvény 37. § *c*) és  
*d*) pontjában,  
a 4. alcím tekintetében a Rendőrségről szóló 1994. évi XXXIV. törvény 100. § (1) bekezdés  
*h*) pontjában,  
az 5. alcím tekintetében a büntetés-végrehajtási szervezetről szóló 1995. évi CVII. törvény 35.  
§ (1) bekezdés *b*) pontjában,  
a 6. alcím tekintetében a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési  
nyilvántartási rendszerről szóló 2012. évi II. törvény 250. § (1) bekezdés *c*) pontjában,  
a 7. alcím tekintetében az elektronikus ügyintézés és a bizalmi szolgáltatások általános  
szabályairól szóló 2015. évi CCXXII. törvény 105. § (2) bekezdés *c*) pontjában,  
a 8. alcím tekintetében a létfontosságú rendszerek és létesítmények azonosításáról,  
kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 14. § *b*) és *h*) pontjában,  
a 9. alcím tekintetében a temetőkről és a temetkezésről szóló 1999. évi XLIII. törvény 41. §  
(1) bekezdés *e*) pontjában,  
a 10. alcím tekintetében a létfontosságú rendszerek és létesítmények azonosításáról,  
kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 14. § *a*) pontjában,  
a 11. alcím tekintetében az államháztartásról szóló 2011. évi CXCV. törvény 109. § (1)  
bekezdés 15a. pontjában kapott felhatalmazás alapján,  
a 12. alcím tekintetében az állami és önkormányzati szervek elektronikus  
információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés *g*) pontjában,  
a 13. alcím tekintetében az állami és önkormányzati szervek elektronikus  
információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés *a*)-*c*), *h*) és *i*)  
pontjában,  
a 14. alcím tekintetében a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló  
1992. évi LXVI. törvény 47. § (1) bekezdés *a*), *e*) és *g*) pontjában,  
a 15. alcím tekintetében a kéményseprő-ipari tevékenységről szóló 2015. évi CCXI. törvény  
8. § (1) bekezdésben kapott felhatalmazás alapján,  
a 16. alcím tekintetében a védelmi és biztonsági célú beszerzésekről szóló 2016. évi XXX.  
törvény 172. § (1) bekezdés *b*) pontjában,  
a 17. alcím tekintetében az elektronikus ügyintézés és a bizalmi szolgáltatások általános  
szabályairól szóló 2015. évi CCXXII. törvény 105. § (1) bekezdés *c*) és *g*) pontjában, (2)  
bekezdés *c*) pontjában  
kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott  
feladatkörében eljárva a következőket rendeli el:

#### **1. A külföldre utazásról szóló 1998. évi XII. törvény végrehajtásáról szóló 101/1998. (V. 22.) Korm. rendelet módosítása**

##### **1. §**

A külföldre utazásról szóló 1998. évi XII. törvény végrehajtásáról szóló 101/1998. (V. 22.) Korm. rendelet (a továbbiakban: Utvvr.) 13. § (2) bekezdése helyébe a következő rendelkezés lép:

„(2) Az útlevél iránti kérelemről az általános hatáskörű útlevélhatóság, a járási hivatal vagy a konzuli tisztviselő – az egészségi állapot miatti meghatalmazotti eljárás kivételével – a kérelemnek megfelelő adattartalmú, elektronikus kérelmet állít elő, amely tartalmazza a kérelmező saját kezű aláírását, ha 12. életévét betöltötte, valamint nem írásképtelen vagy írástudatlan, továbbá arcképmását és – az Utv. 7. § (4) bekezdésében foglalt kivétellel – a tagállamok által kiállított útlevélek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló, 2004. december 13-i 2252/2004/EK tanácsi rendelet 1. cikk (2) bekezdés második mondata szerinti biometrikus adatát (a továbbiakban: második biometrikus adat), továbbá a kérelmező birtokában lévő előző útlevél érvénytelenítésére, visszahagyására vonatkozó bejegyzést is.”

## 2. §

Az Utvvr. 17. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) Az úti okmány iránti kérelem előterjesztésekor a kérelmező a kérelmezett úti okmány adattartalmát képező személyes adatait, azok ellenőrzésére szolgáló okiratokat, lakcímét, illetve értesítési címét, továbbá arcképmását és saját kezű aláírását, ha 12. életévét betöltötte, valamint nem írásképtelen vagy írástudatlan, köteles az eljáró útlevélhatóság rendelkezésére bocsátani. Az írásképtelen vagy írástudatlan, illetőleg a 12. életévét be nem töltött kérelmező útlevélének aláírás rovata bejegyzést nem tartalmaz. Az Utv. 7. § (4) bekezdésében foglalt kivétellel a kérelmező az útlevél kérelmezésekor köteles a második biometrikus adatot az útlevélhatóság rendelkezésére bocsátani. A kiskorú vagy gondnokság alatt álló személy kérelmét törvényes képviselője nyújtja be és írja alá.”

## **2. Az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelet módosítása**

## 3. §

Az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelet [a továbbiakban: 92/2010. (III. 31.) Korm. rendelet] 3. § (1) és (2) bekezdése helyébe a következő rendelkezés lép:

„(1) A minősített adatot kezelő szerv vagy a gazdálkodó szervezet a „Szigorúan titkos!”, a „Titkos!”, illetve a „Bizalmas!” minősítési szintű adatok kezelésére jogosító telephely biztonsági tanúsítvány kiadására irányuló eljárás megindítását az 1. mellékletben meghatározott adattartalommal a Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) elnöke által rendszeresített és az NBF honlapján közzétett Cég-adatlap, a 4. § (4) bekezdésében foglaltak alapján az érintett személyek által kitöltött biztonsági kérdőív, valamint a 6. § (2) bekezdés c) pontjában meghatározott feltétel teljesítéséhez szükséges Adatlap egyszerre történő megküldésével kezdeményezi az NBF-nél. Telephely biztonsági

tanúsítvány kizárólag olyan gazdálkodó szervezetnek adható ki, amelynek alapítása és a Cég-adatlap benyújtása között legalább két év eltelt.

(2) A minősített adatot kezelő szerv vagy a gazdálkodó szervezet a „Szigorúan titkos!”, a „Titkos!”, illetve a „Bizalmas!” minősítési szintű adatok kezelésére jogosító egyszerűsített telephely biztonsági tanúsítvány kiadására irányuló eljárás megindítását a 2. mellékletben meghatározott adattartalommal az NBF elnöke által rendszeresített és az NBF honlapján közzétett Cég-adatlap, a 4. § (5) bekezdésében foglaltak alapján az érintett személyek által kitöltött biztonsági kérdőív, valamint a 6. § (4) bekezdés *b*) pontjában meghatározott feltétel teljesítéséhez szükséges Adatlap egyszerre történő megküldésével kezdeményezi az NBF-nél. Telephely biztonsági tanúsítvány kizárólag olyan gazdálkodó szervezetnek adható ki, amelynek alapítása és a Cég-adatlap benyújtása között legalább két év eltelt.”

#### 4. §

A 92/2010. (III. 31.) Korm. rendelet 4. § (4)-(6) bekezdése helyébe a következő rendelkezés lép:

„(4) A 3. § (1) bekezdése szerinti esetben az iparbiztonsági ellenőrzés során a nemzetbiztonsági szolgálat végrehajtja a gazdálkodó szervezet ügyvezetését ellátó személyek, a gazdálkodó szervezet legalább öt százalékot meghaladó vagyoni hozzájárulással rendelkező tagja, alapítója, részvényese, a kijelölésre kerülő biztonsági vezető, valamint a titkos ügykezelő és helyettese, a rendszerbiztonsági felügyelő, a rendszeradminisztrátor, továbbá a minősített szerződésben való igazolt részvétel esetén annak előkészítésében és végrehajtásában érintett személyek nemzetbiztonsági ellenőrzését.

(5) A 3. § (2) bekezdése szerinti esetben az iparbiztonsági ellenőrzés során a nemzetbiztonsági szolgálat végrehajtja a gazdálkodó szervezet ügyvezetését ellátó személyek, a gazdálkodó szervezet legalább öt százalékot meghaladó vagyoni hozzájárulással rendelkező tagja, alapítója, részvényese, a kijelölésre kerülő biztonsági vezető, valamint a minősített szerződésben való igazolt részvétel esetén annak előkészítésében és végrehajtásában érintett személyek nemzetbiztonsági ellenőrzését.

(6) A (4) vagy (5) bekezdésben meghatározott személyek a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 2. számú mellékletében szereplő biztonsági kérdőívet a nemzetbiztonsági ellenőrzés és a felülvizsgálati eljárás során a biztonsági kérdőív kitöltésének eljárási szabályairól, valamint a nemzetbiztonsági ellenőrzéssel összefüggésben a lényeges adatokban bekövetkezett változás bejelentésének rendjéről szóló kormányrendeletben foglaltak szerint töltik ki az NBF honlapján közzétett Tájékoztatóban foglaltak szerint azzal, hogy biztonsági megbízott alatt az NBF kijelölt munkatársát kell érteni. A nemzetbiztonsági ellenőrzést az NBF elnöke kezdeményezi.”

#### 5. §

A 92/2010. (III. 31.) Korm. rendelet 10/A. § (2) bekezdése helyébe a következő rendelkezés lép:

„(2) Az (1) bekezdés szerinti telephely biztonsági tanúsítvány kiadására irányuló eljárás megindítását a gazdálkodó szervezet a 2. mellékletben meghatározott adattartalommal az NBF elnöke által rendszeresített és az NBF honlapján közzétett Cég-adatlap, a 4. § (5) bekezdésben foglaltak alapján az érintett személyek által kitöltött biztonsági kérdőív, valamint a 6. § (4) bekezdés *b*) pontjában meghatározott feltétel teljesítéséhez szükséges Adatlap egyszerre történő megküldésével kezdeményezi az NBF-nél. Az (1) bekezdés szerinti telephely

biztonsági tanúsítvány kizárólag olyan gazdálkodó szervezetnek adható ki, amelynek alapítása és a Cég-adatlap benyújtása között legalább két év eltelt.”

## 6. §

A 92/2010. (III. 31.) Korm. rendelet

a) 1. melléklet 1. pont 1.9. alpontjában és a 2. melléklet 1.9. alpontjában a „jelenlegi tulajdonosainak megnevezése” szövegrész helyébe a „legalább öt százalékot meghaladó vagyoni hozzájárulással rendelkező tagjának, alapítójának, részvényesének természetes személyazonosító adatai”,

b) 1. melléklet 2. pont 2.2. alpontjában és a 2. melléklet 2. pont 2.2. alpontjában az „a vezetőtestület tagjainak” szövegrész helyébe az „az ügyvezetést ellátó személyek” szöveg lép.

### **3. A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet módosítása**

## 7. §

(1) A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet [a továbbiakban: 161/2010. (V. 6.) Korm. rendelet] 4. § (1) bekezdés *i*) pontja helyébe a következő rendelkezés lép:

*(Az NBF általános feladatkörében:)*

„*i*) együttműködik az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 19. § (1) bekezdése szerinti eseménykezelő központtal.”

(2) A 161/2010. (V. 6.) Korm. rendelet 4. § (4) bekezdés *e*) pontja helyébe a következő rendelkezés lép:

*(Az NBF a nemzeti TEMPEST hatóság feladatainak keretén belül)*

„*e*) a TEMPEST mérések alapján zónába sorolja a rendszer környezetét,”

## 8. §

A 161/2010. (V. 6.) Korm. rendelet 5. § (1) bekezdés *a*) pontja helyébe a következő rendelkezés lép:

*(Magyarország nemzetközi kötelezettségvállalásainak teljesítése érdekében)*

„*a*) a honvédelemért felelős miniszter látja el a NATO Központi Rejtjel Elosztó Hatóság feladatait,”

## 9. §

A 161/2010. (V. 6.) Korm. rendelet 8. § g) pontja helyébe a következő rendelkezés lép:

*(A minősített adatot elektronikus rendszeren kezelő szerv biztonsági vezetője)*

„g) folyamatos kapcsolatot tart az lbtv. 19. § (1) bekezdése szerinti eseménykezelő központtal a használt rendszerek hálózati biztonsága vonatkozásában.”

### **10. §**

A 161/2010. (V. 6.) Korm. rendelet 22. §-a a következő (6)-(7) bekezdéssel egészül ki:

„(6) Állami szervek esetében, ha a legfeljebb „Titkos!” minősítési szintű nemzeti minősített adatokat kezelő rendszer és elemei 1. kategóriájú biztonsági tároló használatával engedélyezett II. osztályú biztonsági területen helyezkednek el, a rendszer minősített adathordozói tekintetében biztonsági tárolónak, illetve zárnak tekinthető, ha az adathordozóhoz való hozzáférést legalább 1. kategóriájú tárolóval azonos szintű védelmet nyújtó zárható burkolattal vagy az adathordozó eltávolítását legalább 1. kategóriájú zárszerkezet alkalmazásával akadályozzák meg.

(7) A nemzeti minősített adatot kezelő elektronikus rendszert biztonsági területen kívül, adminisztratív zónában, a biztonsági vezető által megjelölt helyszínen, kizárólag személyes felügyelet alatt lehet üzemeltetni. Nemzeti „Titkos!” vagy „Szigorúan titkos!” elektronikus rendszer esetén a rendszer elemeinek meg kell felelnie a TEMPEST követelményeknek.”

### **11. §**

A 161/2010. (V. 6.) Korm. rendelet 28. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) A rendszer elemeit az adminisztratív zónából, valamint a biztonsági területről nem üzemeltetés céljából kivinni kizárólag az adathordozó – és minden más, adat visszanyerésére alkalmas részegység – eltávolítását és biztonsági területen hagyását követően szabad, kivéve a más adminisztratív zónába vagy biztonsági területre történő szállítást.”

### **12. §**

A 161/2010. (V. 6.) Korm. rendelet a következő 34/A. §-sal egészül ki:

„34/A. § (1) A minősített adatot elektronikus rendszeren kezelő szerv az NBF által jóváhagyott operációs rendszert alkalmaz.

(2) Az operációs rendszert havonta frissíteni kell.”

### **13. §**

A 161/2010. (V. 6.) Korm. rendelet 38. § (3) bekezdése helyébe a következő rendelkezés lép:

„(3) A minősített adatot elektronikus rendszeren kezelő szerv a biztonsági másolatot a rendszeren kezelhető minősített adatok legmagasabb minősítési szintjének megfelelő biztonsági körülmények között, a rendszerben elkülönítve vagy a rendszertől elkülönített módon tárolja.”

### **14. §**

A 161/2010. (V. 6.) Korm. rendelet 39. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) A minősített adatot elektronikus rendszeren kezelő szerv a vírusok és más rosszindulatú szoftverek azonosítására és eltávolítására az NBF által jóváhagyott vírusvédelmi szoftvert alkalmaz.”

### **15. §**

(1) A 161/2010. (V. 6.) Korm. rendelet 45. § (2) bekezdés *a*) pontja helyébe a következő rendelkezés lép:

*(A rejtjeltevékenységet folytató szerv a rendszeresítési engedély iránti kérelemben benyújtja:)*

„*a*) a rejtjelző eszköz két működőképes példányát vagy jellegéből adódóan központi elemét,”

(2) A 161/2010. (V. 6.) Korm. rendelet 45. § (2) bekezdése a következő *g*) ponttal egészül ki:

*(A rejtjeltevékenységet folytató szerv a rendszeresítési engedély iránti kérelemben benyújtja:)*

„*g*) a rejtjelző eszköz működtetési szabályzatát, kezelési utasítását és a rejtjelző eszköz alkalmazásához szükséges egyéb dokumentumokat.”

### **16. §**

A 161/2010. (V. 6.) Korm. rendelet 46. § (3) bekezdése helyébe a következő rendelkezés lép:

„(3) Az NBF a rendszeresítési engedély kiadásába szakértőként az Információs Hivatalt vonhatja be a nemzetbiztonsági szolgálatokról szóló törvényben foglalt feladatai végrehajtása érdekében.”

### **17. §**

A 161/2010. (V. 6.) Korm. rendelet 48. § (1) bekezdés *b*) pontja helyébe a következő rendelkezés lép:

*(Az NBF engedélye szükséges továbbá:)*

„*b*) a rejtjelző eszközzel kapcsolatos fejlesztési, gyártási, beszerzési tevékenységhez,”

### **18. §**

A 161/2010. (V. 6.) Korm. rendelet 54. § (2) bekezdése helyébe a következő rendelkezés lép:

„(2) A rejtjeltevékenységgel kapcsolatos belső ellenőrzésre a minősített adatot elektronikus rendszeren kezelő szerv vezetője, a biztonsági vezető, rejtjelfelügyelő vagy a rejtjelfelügyelet vezetője és a szerv rejtjelszabályzatában meghatározott további személyek jogosultak.”

### **19. §**

A 161/2010. (V. 6.) Korm. rendelet 56. § (1) és (2) bekezdése helyébe a következő rendelkezés lép:

„(1) Az NBF a rendszerbiztonsági felügyelet és rejtjelfelügyelet részére évenként képzést tart az elektronikus és a rejtjelbiztonsággal kapcsolatban.

(2) A rendszerbiztonsági felügyelő vagy a rendszerbiztonsági felügyelet vezetője és a rejtjelfelügyelő vagy a rejtjelfelügyelet vezetője, valamint az általa kijelölt személy a képzésen részt vesz.”

## 20. §

A 161/2010. (V. 6.) Korm. rendelet 57. §-a helyébe a következő rendelkezés lép:

„57. § A rendszer felhasználói részére a képzést a rendszerbiztonsági felügyelet és a rejtjelfelügyelet legalább két évente megtartja.”

## 21. §

A 161/2010. (V. 6.) Korm. rendelet 50. § (1) és (2) bekezdésében a „határozat” szövegrész helyébe a „dokumentum” szöveg lép.

## 22. §

Hatályát veszti a 161/2010. (V. 6.) Korm. rendelet

a) 16. alcíme,

b) 48. § (1) bekezdés e) pontja.

### **4. A terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) Korm. rendelet módosítása**

## 23. §

A terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) Korm. rendelet 3. § (1) bekezdése a következő *l)* ponttal egészül ki:

*(A TEK az Rtv. 7/E. § (1) bekezdés a) pontjában, b) pont ba) alpontjában és c) pontjában, valamint (3), (5) és (6) bekezdésében meghatározott feladatok ellátása érdekében)*

„*l)* ellátja a felderítési, felszámolási és személyvédelmi feladatkörében felmerülő vegyi, biológiai vagy nukleáris veszélyek felderítésére és elhárítására irányuló tevékenységet, illetve annak koordinálását, ennek keretében végzi különösen az objektumok, járművek, útvonalak és műveleti helyszínek vegyi, biológiai vagy nukleáris veszélyek felderítésére és elhárítására irányuló átvizsgálását.”

## 24. §

Hatályát veszti a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) Korm. rendelet 2. § (2) bekezdése.

**5. A büntetés-végrehajtási szervezet részéről a központi államigazgatási szervek és a rendvédelmi szervek irányában fennálló egyes ellátási kötelezettségekről, a termékek és szolgáltatások átadás-átvételének és azok ellentételezésének rendjéről szóló 44/2011. (III. 23.) Korm. rendelet módosítása**

**25. §**

A büntetés-végrehajtási szervezet részéről a központi államigazgatási szervek és a rendvédelmi szervek irányában fennálló egyes ellátási kötelezettségekről, a termékek és szolgáltatások átadás-átvételének és azok ellentételezésének rendjéről szóló 44/2011. (III. 23.) Korm. rendelet 1. § (1) bekezdésében a „szociális intézmények” szövegrész helyébe a „szociális intézmények, a tankerületi központok” szöveg lép.

**6. Az egyes közlekedési szabálysértések miatt alkalmazandó szabálysértési pénzbírság, illetve helyszíni bírság kötelező mértékéről, valamint a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvénnyel összefüggő egyes kormányrendeletek módosításáról szóló 63/2012. (IV. 2.) Korm. rendelet módosítása**

**26. §**

Az egyes közlekedési szabálysértések miatt alkalmazandó szabálysértési pénzbírság, illetve helyszíni bírság kötelező mértékéről, valamint a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvénnyel összefüggő egyes kormányrendeletek módosításáról szóló 63/2012. (IV. 2.) Korm. rendelet 1. melléklet

- a) 1. sorában a „0,50‰” szövegrész helyébe a „0,30‰” szöveg, a „0,30mg/l-t” szövegrész helyébe a „0,15 mg/l-t” szöveg,
- b) 2. sorában a „mértéke 0,50‰” szövegrész helyébe a „mértéke 0,30‰” szöveg, a „0,80‰” szövegrész helyébe a „0,50‰” szöveg, a „0,30 mg/l-nél” szövegrész helyébe a „0,15 mg/l-nél” szöveg, az „a 0,50 mg/l-t” szövegrész helyébe az „a 0,25 mg/l-t” szöveg,
- c) 3. sorában a „0,80‰” szövegrész helyébe a „0,50‰” szöveg és a „0,50 mg/l-t” szövegrész helyébe a „0,25 mg/l-t” szöveg

lép.

**7. Egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) Korm. rendelet módosítása**

**27. §**

Egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) Korm. rendelet a következő 4/B. §-sal egészül ki:

„4/B. § A 4. § g) pont ga) alpontja szerinti esetben a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter a kijelölés szerinti feladatát az Alkotmányvédelmi Hivatal tekintetében az Alkotmányvédelmi Hivatal útján látja el.”

**8. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet módosítása**

## 28. §

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet [a továbbiakban: 65/2013. (III. 8.) Korm. rendelet] 4. §-a helyébe a következő rendelkezés lép:

„4. § (1) A kijelölő hatóság a nemzeti létfontosságú rendszerelemmé történő kijelölésről, valamint a kijelölés visszavonásáról szakhatóság bevonásával dönt. Ha kijelölő hatóságként a hivatásos katasztrófavédelmi szerv központi, területi vagy helyi szerve jár el, a horizontális kritériumoknak teljesülése fennállásának a kérdését a hatósági eljárás során a kijelölő hatóság vizsgálja.

(2) A nemzeti létfontosságú rendszerelemmé történő kijelölésre, valamint a kijelölés visszavonására vonatkozó eljárásban előzetes szakhatósági állásfoglalásnak nincs helye.

(3) A kijelölő hatóság a határozatában:

a) jóváhagyja az üzemeltető azonosítási jelentését és a rendszerelemet – feltéve, hogy az ágazati kritériumok közül és a szakhatóság állásfoglalása, a (2) bekezdés szerinti esetben a hatóság döntése alapján az 1. mellékletben felsorolt horizontális kritériumok közül legalább egy-egy bekövetkezésének lehetősége fennáll – nemzeti létfontosságú rendszerelemként jelöli ki és elrendeli nyilvántartásba vételét,

b) jóváhagyja az üzemeltető azonosítási jelentését és a kijelölést visszavonja, valamint elrendeli a nyilvántartásból való törlést,

c) a kijelölésre, kijelölés visszavonására irányuló javaslatot elutasítja, vagy legfeljebb 90 napos határidő tűzésével és a feltárt hibák, hiányosságok tételes megjelölésével új azonosítási jelentés benyújtását írja elő, vagy

d) jóváhagyja, hogy az üzemeltető egyetlen rendszerelemet sem azonosított lehetséges létfontosságú rendszerelemként,

e) az a) pontban meghatározottakkal egyidejűleg rendelkezik az üzemeltető felvételéről az alapvető szolgáltatásokat nyújtó szereplők jegyzékébe, ha a nemzeti létfontosságú rendszerelem tekintetében megvalósulnak az Lrtv. 2/A. § (2) bekezdésében foglaltak, vagy

f) a b) pontban foglaltak teljesülése esetén elrendeli az üzemeltető törlését az alapvető szolgáltatásokat nyújtó szereplők jegyzékéből.

(4) A nemzeti létfontosságú rendszerelemmé történő kijelölés, valamint a visszavonására vonatkozó eljárásban a kérelem kormányablaknál történő előterjesztése kizárt.

(5) A kijelölő hatóság a nemzeti létfontosságú rendszerelemmé történő kijelölés tényéről és időpontjáról, valamint a kijelölés visszavonásának tényéről és időpontjáról tájékoztatja az egységes digitális rádiótávközlő rendszer (a továbbiakban: EDR) kormányzati célú hírközlési szolgáltatóját. A szolgáltató a tudomására jutott adatokat harmadik személy számára nem teheti hozzáférhetővé.

(6) A nemzeti létfontosságú rendszerelemmé történő kijelölés, valamint a visszavonására vonatkozó eljárásban kétszeri hiánypótlásra történő felszólításnak van helye.”

## 29. §

A 65/2013. (III. 8.) Korm. rendelet 5. §-a helyébe a következő rendelkezés lép:

„5. § (1) Ha az üzemeltető által lefolytatott azonosítási eljárás alapján elkészített azonosítási jelentésben foglaltakkal vagy a javaslattevő hatóság európai létfontosságú rendszerelemmé történő kijelölésre irányuló kezdeményezésével a katasztrófák elleni védekezésért felelős miniszter nem ért egyet, a kijelölő hatóság köteles megvizsgálni a nemzeti létfontosságú

rendszerlemmé történő kijelölés kérdését, és a jogszabályban meghatározott feltételek fennállása esetén dönt a nemzeti létfontosságú rendszerlemmé történő kijelölésről.

(2) Ha az Európai Gazdasági Térségről szóló megállapodásban részes más állam (a továbbiakban: EGT-állam) európai létfontosságú rendszerlemmé történő kijelölésre irányuló kezdeményezésével a katasztrófák elleni védekezésért felelős miniszter nem ért egyet, erről tájékoztatja a kezdeményező államot.

(3) Ha az EGT-állam európai létfontosságú rendszerlemmé történő kijelölés visszavonására irányuló kezdeményezésével, illetve az üzemeltető európai létfontosságú rendszerlemmé történő kijelölés visszavonására irányuló kérelmével a katasztrófák elleni védekezésért felelős miniszter egyetért, az Lrtv. 3. § (3) bekezdése szerinti szabályok megfelelő alkalmazásával kell eljárni. A kijelölő hatóság az Lrtv. 3. § (4) bekezdése megfelelő alkalmazásával az európai létfontosságú rendszerlemmé való kijelölést visszavonja, valamint a jogszabályban meghatározott feltételek fennállása esetén dönt a nemzeti létfontosságú rendszerlemmé történő kijelölésről.

(4) Ha az üzemeltető európai létfontosságú rendszerlemmé történő kijelölés visszavonására irányuló kérelmével a katasztrófák elleni védekezésért felelős miniszter nem ért egyet, a kijelölő hatóság tájékoztatja az üzemeltetőt a kijelölés fenntartásáról. Ha a visszavonást EGT-állam kezdeményezi, az Lrtv. 3. § (3)–(4) bekezdése szerinti szabályok megfelelő alkalmazásával kell eljárni.

(5) A katasztrófák elleni védekezésért felelős miniszter az európai létfontosságú rendszerlemmé történő kijelölés folyamatában a horizontális kritériumok teljesülésének lehetőségét vizsgálja.

(6) Ha az európai létfontosságú rendszerlemmé történő kijelölés, vagy a kijelölés visszavonása kérdésében az ágazatért felelős miniszter és a katasztrófák elleni védekezésért felelős miniszter ellentétes álláspontot képvisel, a végleges álláspontról a Kormány dönt.

(7) Az európai létfontosságú rendszerlemmé történő kijelölés, valamint a kijelölés visszavonására vonatkozó eljárásban a kérelem kormányablaknál történő előterjesztése kizárt.

(8) A kijelölő hatóság az európai létfontosságú rendszerlemmé történő kijelölés tényéről és időpontjáról, valamint a kijelölés visszavonásának tényéről és időpontjáról tájékoztatja az EDR kormányzati célú hírközlési szolgáltatóját. A szolgáltató a tudomására jutott adatokat harmadik személy számára nem teheti hozzáférhetővé.

(9) Az európai létfontosságú rendszerlemmé történő kijelölés, valamint a visszavonására vonatkozó eljárásban kétszeri hiánypótlásra történő felszólításnak van helye.”

### **30. §**

A 65/2013. (III. 8.) Korm. rendelet 7. § (5) bekezdése helyébe a következő rendelkezés lép:

„(5) Ha az üzemeltetői biztonsági tervet a (2)-(3) bekezdés vagy az Lrtv. 6. § (6) bekezdése alapján módosítani szükséges, akkor annak módosítással érintett részét, vagy jelentős tartalmi módosítás esetén a módosításokkal egységes szerkezetbe foglalt üzemeltetői biztonsági tervet az üzemeltető haladéktalanul megküldi tartalmi és formai ellenőrzésre a kijelölő hatóságnak. Az ellenőrzés határideje 30 nap. A (2)-(3) bekezdés alapján módosított üzemeltetői biztonsági tervet az ágazati kijelölő hatóság a tartalmi és formai ellenőrzést követően megküldi a nyilvántartó hatóság részére.”

### **31. §**

A 65/2013. (III. 8.) Korm. rendelet 8. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) A honvédelmi létfontosságú rendszerelemek kivételével, a létfontosságú rendszerelemek védelmét a helyszíni ellenőrzés lefolytatására jogosult szervek a hivatásos katasztrófavédelmi szerv központi szervének koordinálásával ütemezett módon, éves ellenőrzési terv alapján összehangoltan is ellenőrzik, oly módon, hogy a létfontosságú rendszerelem legalább 5 évente kerüljön ellenőrzésre. Az éves ellenőrzési tervet a hivatásos katasztrófavédelmi szerv központi szerve a tárgyévvel megelőző év november 30-ig állítja össze.”

**9. A temetőkről és a temetkezésről szóló 1999. évi XLIII. törvény végrehajtásáról szóló 145/1999. (X. 1.) Korm. rendelet, valamint az egészségügyi szolgáltatások Egészségbiztosítási Alapból történő finanszírozásának részletes szabályairól szóló 43/1999. (III. 3.) Korm. rendelet módosításáról szóló 379/2013. (X. 25.) Korm. rendelet módosítása**

**32. §**

A temetőkről és a temetkezésről szóló 1999. évi XLIII. törvény végrehajtásáról szóló 145/1999. (X. 1.) Korm. rendelet, valamint az egészségügyi szolgáltatások Egészségbiztosítási Alapból történő finanszírozásának részletes szabályairól szóló 43/1999. (III. 3.) Korm. rendelet módosításáról szóló 379/2013. (X. 25.) Korm. rendelet 33. § (2) bekezdésében a „2019. január 1-jén” szövegrész helyébe a „2021. január 1-jén” szöveg lép.

**10. Egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendelet módosítása**

**33. §**

Az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendelet 3. §-a helyébe a következő rendelkezés lép:

„3. § A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság és szervei létfontosságú rendszerei vonatkozásában a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 8. §-a szerinti ellenőrzést koordináló és a helyszíni ellenőrzést lefolytató szerv a katasztrófák elleni védekezésért felelős miniszter, aki az általa kijelölt, ellenőrzési feladatokat ellátó szervezeti egység közreműködésével látja el a feladatot.”

**11. A 2014-2020 közötti programozási időszakban a Belső Biztonsági Alapból és a Menekültügyi, Migrációs és Integrációs Alapból származó támogatások felhasználásáról szóló 135/2015. (VI. 2.) Korm. rendelet módosítása**

**34. §**

A 2014-2020 közötti programozási időszakban a Belső Biztonsági Alapból és a Menekültügyi, Migrációs és Integrációs Alapból származó támogatások felhasználásáról szóló 135/2015. (VI. 2.) Korm. rendelet [a továbbiakban: 135/2015. (VI. 2.) Korm. rendelet] 2. § 10. pontja helyébe a következő rendelkezés lép:

„10. kiválasztási eljárás: a Nemzeti Programban megjelölt célkitűzések elérése érdekében történő forráselosztás;”

### 35. §

A 135/2015. (VI. 2.) Korm. rendelet 4. §-a a következő (5) és (6) bekezdéssel egészül ki:

„(5) A Felelős Hatóság a partnerség elvével összhangban gondoskodik a pályázati kiírások egyeztetéséről.

(6) A Felelős Hatóság az adott pénzügyi évre vonatkozó szakmai és a pénzügyi helyszíni ellenőrzéseit a vonatkozó jogszabályok rendelkezéseinek figyelembevételével az adott pénzügyi év október 15-ig folytatja le.”

### 36. §

A 135/2015. (VI. 2.) Korm. rendelet 7. § (2) bekezdése helyébe a következő rendelkezés lép:

„(2) A Monitoring Bizottság ellátja a Nemzeti Programok teljesülésének nyomon követését és javaslatot tesz az Európai Bizottság részére megküldendő jelentések tartalmára.”

### 37. §

A 135/2015. (VI. 2.) Korm. rendelet

a) 11. § (5) bekezdésében „a szabálytalansági eljárás megindításával” szövegrész helyébe „a szabálytalansági gyanú észlelésével” szöveg,

b) 1. melléklet 1.4.2. pontjában a „25%-át” szövegrész helyébe a „30%-át” szöveg lép.

### 38. §

Hatályát veszti a 135/2015. (VI. 2.) Korm. rendelet

a) 2. § 13. pontja,

b) 3. § c) pontja,

c) 4. Munkaprogram alcíme,

d) 17. § (1) bekezdése.

## **12. A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet módosítása**

### 39. §

A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet [a továbbiakban: 186/2015. (VII. 13.) Korm. rendelet] 2. § g) pontja helyébe a következő rendelkezés lép:

*(Az Ibtv. 11. § (2) és (3) bekezdése szerinti szolgáltatási tevékenysége keretében a központi szolgáltató)*

„g) az elektronikus információs rendszereket érintő biztonsági események kezelése során  
ga) tájékoztatja az Ibtv. 19. § (1)-(3) bekezdése szerinti, feladat- és hatáskörrel rendelkező eseménykezelő központot az azonosított biztonsági eseményekről és fenyegetettségekről,  
gb) biztosítja a biztonsági események azonosításához, elemzéséhez és kezeléséhez szükséges, bizonyíték értékű információkat az Ibtv. 19. § (1)-(3) bekezdése szerinti, feladat- és hatáskörrel rendelkező eseménykezelő központ részére, valamint  
gc) közreműködik az Ibtv. 19. § (1)-(3) bekezdése szerinti eseménykezelő központok által végzett informatikai biztonsági eseménykezelésben a biztonsági eseményről szóló adatszolgáltatással, vizsgálat elvégzésével, illetve az Ibtv. 19. § (1)-(3) bekezdése szerinti eseménykezelő központok által elrendelt biztonságnövelő intézkedések végrehajtásával.”

#### 40. §

A 186/2015. (VII. 13.) Korm. rendelet 2/A. §-a helyébe a következő rendelkezés lép:

„2/A. § A központi szolgáltató köteles a Kormányzati Adatközpont révén nyújtott szolgáltatásai körében az azt igénylő ügyfelei számára biztosítani a korai figyelmeztető rendszerhez való kapcsolódást az ahhoz szükséges, a következő műszaki feltételek megteremtésével és fenntartásával:

- a) a hálózati forgalom másolatának átadásával,
- b) az internet felé menő, illetve onnan érkező hálózati forgalom SSL/TLS csatornáinak feloldása az SSL/TLS csatornák terminálásával vagy SSL/TLS átjáró megvalósításával,
- c) a korai figyelmeztető rendszer működtetőjével az ügyfelek kapcsolódásának kialakításával.”

#### 41. §

A 186/2015. (VII. 13.) Korm. rendelet 3. §-a helyébe a következő rendelkezés lép:

„3. § A központi szolgáltató a szolgáltatások tekintetében, különösen a 2. § g) pontja szerinti tevékenysége keretében együttműködik

- a) a Nemzeti Elektronikus Információbiztonsági Hatósággal,
- b) az Ibtv. 19. § (1)-(3) bekezdése szerinti eseménykezelő központokkal,
- c) az Ibtv. felhatalmazása alapján az elektronikus információbiztonsággal kapcsolatban hatósági feladatok ellátására kijelölt szervezetekkel, valamint
- d) a korai figyelmeztető rendszer működtetőjével.”

#### 42. §

A 186/2015. (VII. 13.) Korm. rendelet 4. §-ában az „a kormányzati” szövegrész helyébe az „az Ibtv. 19. § (1) bekezdése szerinti” szöveg lép.

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

#### 43. §

Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet (a továbbiakban: 187/2015. (VII. 13.) Korm. rendelet) 2. alcíme helyébe a következő rendelkezés lép:

*„2. Az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóság*

2. § (1) Az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóságként (a továbbiakban: hatóság) a Kormány az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 14. § (1) bekezdése alapján a Nemzetbiztonsági Szakszolgálatot jelöli ki.

A hatósági jogköröket a Szakszolgálat szervezetében működő Nemzeti Kibervédelmi Intézet (a továbbiakban: Kibervédelmi Intézet) gyakorolja.

(2) A hatóság közigazgatási hatósági jogkörében eljárva kizárólag a jogszabályoknak van alávetve, hatósági eljárása során és hatósági döntéseinek tartalmával összefüggésben – a feladat elvégzésére vagy a mulasztás pótlására irányuló utasítás kivételével – nem utasítható.”

#### 44. §

A 187/2015. (VII. 13.) Korm. rendelet. 4. §-a helyébe a következő rendelkezés lép:

„4. § (1) A hatóság az eljárását lezáró döntésének meghozatala előtt az érintett szervezettel – ha ezt azonnali fenyegetés vagy biztonsági esemény, vagy az érintett szervezet ismételt jogsértő magatartása nem zárja ki – egyeztetést folytat le.

(2) A hatóság hatósági eljárása során elfogadja az elektronikus információs rendszerek biztonságának szempontjából releváns európai vagy nemzetközileg elfogadott szabványok és előírások szerinti tanúsítványok, akkreditációk alkalmazását.”

#### 45. §

A 187/2015. (VII. 13.) Korm. rendelet 3. alcíme a következő 5/A. §-sal egészül ki:

„5/A. § A hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult ellenőrizni minden olyan, az elektronikus információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek. Ennek érdekében jogosult eljárása során független, képesített ellenőrt igénybe venni, és az általa végzett ellenőrzés eredményét figyelembe venni.”

#### 46. §

A 187/2015. (VII. 13.) Korm. rendelet 6. § (1) bekezdés e)-g) pontja helyébe a következő rendelkezés lép:

*(A hatóság)*

„e) szükség szerint konzultációt folytat és együttműködik a rendvédelmi szervekkel, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósággal,

f) jogszabályban meghatározott szempontok szerint, hatósági ellenőrzés keretében lefolytatja a fizikai, logikai és adminisztratív védelmi ellenőrzéseket,  
g) az elektronikus információs rendszerek biztonságáért felelős nemzetközi szervezetekben képviseli Magyarországot.”

#### 47. §

A 187/2015. (VII. 13.) Korm. rendelet 13. §-a helyébe a következő rendelkezés lép:

„13. § (1) A hatóság az információbiztonsági követelmények teljesülése érdekében – határidő kitűzése mellett – felhívja az érintett szervezet vezetőjét az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a biztonsági követelmény megsértése megszüntetésére, jogszabályban meghatározott kötelezettség teljesítésére, az elvárt intézkedés megtételére.

(2) A hatóság azonnali intézkedések megtételére kötelezi az érintett szervezetet, ha az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelmény súlyos biztonsági esemény bekövetkeztével fenyeget. Ezzel összefüggésben fegyelmi felelősség megállapítására tehet javaslatot a munkáltatói jogkör gyakorlója felé.

(3) A hatóság az Ibtv. 19. § (1) bekezdése szerinti eseménykezelő központ értesítése esetén – megfelelő határidő tűzése mellett – felszólítja az érintett szervezetet a jogszabálykövető magatartás folytatására, ennek keretében különösen bejelentési, adatszolgáltatási, együttműködési kötelezettségének teljesítésére.

(4) A hatóság az Ibtv. 16. § (2) bekezdés *b)* pontja, valamint a (3) bekezdés *d)* pontja alapján az 1. mellékletben megjelölt szabálytalanság esetén az ott rögzített mértékben bírságot szabhat ki. A kiszabható bírság ötvenezer forinttól ötmillió forintig terjedhet, amelyet a hatóság határozatának véglegessé válását követő nyolc napon belül kell befizetni a hatóság Magyar Államkincstárnál vezetett számlájára.

(5) Az (1)-(4) bekezdésben foglaltakon túlmenően az eljárás akadályozása, illetve az adatszolgáltatás nem vagy nem megfelelő teljesítése esetén a hatóság hárommillió forintig terjedő bírsággal sújthatja - ismételt jogsértés esetén sújtani köteles - a jogsértő vezető tisztségviselőjét is.

(6) A hatóság a jogkövetkezmények alkalmazása során jogszabályban meghatározottakon túl az alábbi szempontokat veszi figyelembe:

*a)* az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelménynek a biztonsági osztályba sorolás és biztonsági szint szerinti súlyát,

*b)* történt-e súlyos biztonsági esemény, vagy fennállt-e ilyen esemény bekövetkeztének veszélye,

*c)* a biztonsági esemény hatását, vagy lehetséges hatását az érintett szervezetre, vagy más szervezetekre,

*d)* az érintett szervezet magatartását, hatósággal való együttműködését és

*e)* az esemény egyedi, vagy ismételt jellegét.”

#### 48. §

A 187/2015. (VII. 13.) Korm. rendelet 25. § (4)-(5) bekezdése helyébe a következő rendelkezés lép:

„(4) Az (1) bekezdés szerinti hatóság az Ibtv.-ben meghatározott - a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

2/A. §-a alapján kijelölt alapvető szolgáltatásokat nyújtó szereplők elektronikus információs rendszereit érintő - biztonsági esemény bekövetkezése esetén, honlapján tájékoztathatja a nyilvánosságot, illetve a szolgáltatókat határozatban kötelezheti tájékoztatásra, ha saját mérlegelése szerint egy adott biztonsági esemény megelőzéséhez vagy egy már folyamatban lévő biztonsági esemény kezeléséhez szükséges.

(4a) Az (1) bekezdés szerinti hatóság monitorozza a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-ai (EU) 2016/1148 európai parlamenti és tanácsi irányelv (a továbbiakban: Irányelv) hazai alkalmazását, és együttműködik az Irányelvnek való megfelelés vizsgálata érdekében az Ibtv. 19. § (1) bekezdése szerinti eseménykezelő központtal és a 29/A. § szerinti nemzeti egyedüli kapcsolattartó ponttal.

(4b) Az (1) bekezdés szerinti hatóság szükség szerint konzultációt folytat és együttműködik a bűnüldöző szervekkel, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

(5) A BM OKF tájékoztatja a 29/A. § szerinti nemzeti egyedüli kapcsolattartó pontot

a) az alapvető szolgáltatásokat nyújtó szereplők azonosítását lehetővé tevő nemzeti intézkedésekről,

b) az Irányelv szerinti kritikus társadalmi, illetve gazdasági tevékenységek fenntartásához nyújtott alapvető szolgáltatások jegyzékéről,

c) az alapvető szolgáltatásokat nyújtó szereplők jegyzékéről, valamint az érintett ágazat szempontja szerinti jelentőségükről,

d) az adott szolgáltatásra támaszkodó felhasználók számáról, vagy az alapvető szolgáltatásokat nyújtó gazdasági szereplő ellátási szintjéről.”

#### 49. §

A 187/2015. (VII. 13.) Korm. rendelet 29. § (1) bekezdésében az „a kormányzati” szövegrész helyébe a „az Ibtv. 19. § (1) bekezdése szerinti” szöveg lép.

#### 50. §

A 187/2015. (VII. 13.) Korm. rendelet a 12/A. alcímmel egészül ki:

#### ***„12/A. Az elektronikus információs rendszerek biztonságáért felelős nemzeti egyedüli kapcsolattartó pont***

29/A. § (1) A hatóság ellátja az Irányelv szerinti nemzeti egyedüli kapcsolattartó pont feladatait, amelynek keretében

a) biztosítja a hatóságok és az érintett EGT tagállamok hatóságai között folytatott együttműködést,

b) együttműködik az Irányelvnek való megfelelés vizsgálata érdekében az Ibtv. 19. § (1) bekezdése szerinti eseménykezelő központtal, a 25. § (1) bekezdése szerinti hatósággal, az Ekertv. 6/B. § (3) bekezdése szerinti hatósággal, valamint a BM OKF-fel,

c) az Irányelvnek megfelelően azonosított alapvető szolgáltatásokat nyújtó szolgáltatók elektronikus információs rendszerei esetében a megfelelés vizsgálatával összefüggő adatokat, valamint a vizsgálat eredményét megküldi az Európai Bizottság részére,

d) tájékoztatja az érintett tagállamokat az azonosított alapvető szolgáltatásokat nyújtó és a bejelentés-köteles szolgáltatást nyújtó szolgáltatók elektronikus információs rendszereiben bekövetkezett biztonsági eseményről, ha a biztonsági esemény jelentős zavart okozott a szolgáltatás nyújtásában, illetve az Együttműködési csoport részére összefoglaló jelentést küld a biztonsági eseményekről,

- e) együttműködik a magyar és a nemzetközi hálózatbiztonsági szervekkel, különösen az Európai Unió e feladatra létrehozott Együttműködési csoportjával (a továbbiakban: Együttműködési csoport) és az Irányelv által létrehozott CSIRT-ek hálózatával,
- f) szükség szerint konzultációt folytat és együttműködik a rendvédelmi szervekkel, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósággal.
- (2) A nemzeti egyedüli kapcsolattartó pont az (1) bekezdés c) pontjában meghatározott tájékoztatás keretében az alábbi adatokat küldi meg az Európai Bizottság részére:
- a) az alapvető szolgáltatásokat nyújtó szereplők azonosítását lehetővé tevő nemzeti intézkedések,
- b) a kritikus társadalmi, gazdasági tevékenységek fenntartásához nyújtott alapvető szolgáltatások jegyzéke,
- c) az alapvető szolgáltatásokat nyújtó szereplők száma, valamint az érintett ágazat szempontja szerinti jelentőségük,
- d) az adott szolgáltatásra támaszkodó felhasználók száma, vagy az alapvető szolgáltatásokat nyújtó gazdasági szereplő ellátási szintje, valamint
- e) az eseménykezelő központok hatásköréről, és a biztonsági események kezelésére szolgáló eljárásról szóló tájékoztatás.”

## 51. §

A 187/2015. (VII. 13.) Korm. rendelet a 12/B. alcímmel egészül ki:

### ***„12/B. A hatósági eljárás során igénybe vehető független szakértőkre vonatkozó rendelkezések***

- 29/B. § (1) A hatóság naprakész szakértői névjegyzéket vezet az eljárása során igénybe vehető szakértőkről, valamint az elfogadott hazai és nemzetközi sérülékenység-vizsgálati képzést nyújtó intézményekről.
- (2) A névjegyzékbe való bekerüléshez a hatóság évente pályázatot hirdet.
- (3) A pályázati kiírás szakmai előkészítését az eseménykezelő központ végzi, az Ibtv. 19. § (2)-(3) bekezdései szerinti eseménykezelő központok egyetértésével.
- (4) A benyújtásra kerülő pályázatok bíráló bizottság elnöke az eseménykezelő központ, tagjai a hatóság, az Ibtv. 19. § (2)-(3) bekezdései szerinti eseménykezelő központok és az Alkotmányvédelmi Hivatal által delegált szakértők.
- (5) A szakértői névjegyzékbe felvételt nyert pályázók a hatóság által kiadott szakértői tanúsítványt kapnak, amely három évig érvényes.
- (6) Az (1) bekezdés szerinti jegyzéket a hatóság a honlapján közzéteszi.”

## 52. §

A 187/2015. (VII. 13.) Korm. rendelet 32. §-a helyébe a következő rendelkezés lép:

- „32. § (1) A nemzeti egyedüli kapcsolattartó pont a 29/A. § (1) bekezdés d) pontja szerinti stratégiát az elfogadástól számított három hónapon belül küldi meg az Európai Bizottságnak.
- (2) A nemzeti egyedüli kapcsolattartó pont a 29/A. § (2) bekezdés a)-d) pontja szerinti információkat első alkalommal 2018. november 9-éig, ezt követően legalább két évente megküldi az Európai Bizottság részére.
- (3) A nemzeti egyedüli kapcsolattartó pont 2018. augusztus 9-ig, azt követően pedig évente egyszer köteles összefoglaló jelentést benyújtani az Irányelv szerinti együttműködési csoportnak az alapvető szolgáltatásokat nyújtó szolgáltatóktól, valamint a bejelentés-köteles

szolgáltatóktól kapott bejelentésekről, és a jelentésnek tartalmaznia kell a bejelentések számát, a bejelentett biztonsági események jellegét, valamint a hozott intézkedéseket.

(4) A BM OKF első alkalommal 2018. október 31-éig, ezt követően legalább két évente tájékoztatást nyújt a nemzeti egyedüli kapcsolattartó pont részére a 25. § (5) bekezdés szerinti információkról.”

### 53. §

A 187/2015. (VII. 13.) Korm. rendelet az 1. melléklet szerinti melléklettel egészül ki.

### 54. §

A 187/2015. (VII. 13.) Korm. rendelet 29. § (1) bekezdésében az „a kormányzati” szövegrész helyébe a „az Ibtv. 19. § (1) bekezdése szerinti” szöveg lép.

### 55. §

Hatályát veszti a 187/2015. (VII. 13.) Korm. rendelet 1. § 1-3. pontja, 6. § (1) bekezdés *h-n*) pontja, 6. § (1a) bekezdése, valamint 28. §-a.

## **14. A személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól szóló 414/2015. (XII. 23.) Korm. rendelet módosítása**

### 56. §

A személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól szóló 414/2015. (XII. 23.) Korm. rendelet 61. §-a a következő (3) és (4) bekezdéssel egészül ki:

„(3) A személyazonosító igazolvány iránti kérelem személyes előterjesztésekor a konzuli tisztviselő által a kérelmezőről készített arcképmás-felvételezés minimum megfelel az okmányirodák működésének személyi és technikai feltételeiről szóló 58/1999. (XII. 30.) BM rendelet (a továbbiakban: 58/1999. BM rendelet) *6. számú mellékletében* meghatározott képfelvételezési követelményeknek.

(4) A külképviselet rendszeres ügyfélfogadásra állandó jelleggel kialakított hivatali helyiségében az arcképmás konzuli tisztviselő általi felvételezésének külső körülményei az 58/1999. BM rendelet *5. sz. mellékletének* II. pontjában foglalt minimális követelmények figyelembevételével kerülnek kialakításra.”

## **15. A kéményseprő-ipari tevékenységről szóló törvény végrehajtásáról szóló 99/2016. (V. 13.) Korm. rendelet módosítása**

### 57. §

A kéményseprő-ipari tevékenységről szóló törvény végrehajtásáról szóló 99/2016. (V. 13.) Korm. rendelet 4. §-a a következő (12a) bekezdéssel egészül ki:

„(12a) A lakások és helyiségek bérletére, valamint az elidegenítésükre vonatkozó egyes szabályokról szóló 1993. évi LXXVIII. törvény 3. § (1) bekezdése szerinti, a helyi önkormányzat tulajdonát képező ingatlanok címadatait a helyi önkormányzat vagy az ingatlan

vagyonkezelője a kéményseprő-ipari ellátási területekre vonatkozóan megyei bontásban negyedévenként, a negyedév első hónapjának 5. napjáig elektronikusan, szerkeszthető formában átadja a kéményseprő-ipari szervnek, illetve a Kstv. 10. § (3) bekezdés szerinti szolgáltatóknak.”

**16. Az alapvető biztonsági érdeket érintő beszerzések Országgyűlés általi mentesítésének kezdeményezésére vonatkozó feltételekről és eljárásról, valamint az ilyen beszerzések megvalósításakor az ajánlatkérő által érvényesítendő követelményekről szóló 225/2016. (VII. 29.) Korm. rendelet módosítása**

**58. §**

Az alapvető biztonsági érdeket érintő beszerzések Országgyűlés általi mentesítésének kezdeményezésére vonatkozó feltételekről és eljárásról, valamint az ilyen beszerzések megvalósításakor az ajánlatkérő által érvényesítendő követelményekről szóló 225/2016. (VII.29.) Korm. rendelet 5. §-a helyébe a következő rendelkezés lép:

„5. § Az előterjesztő miniszter gondoskodik a mentesítési kérelmek tárgyában hozott országgyűlési bizottsági határozatok, valamint a Kabinet döntéseinek beszerzéséről, továbbá a beszerzett országgyűlési bizottsági határozatokról, valamint a Kabinet döntéseiről nyilvántartást vezet. A nyilvántartásban szerepeltetni kell

a) a mentesítési kérelemnek helyt adó és azt elutasító határozatokat, valamint a határozat számát,

b) a mentesítési kérelmet benyújtó ajánlatkérő nevét,

c) a Vbt. szerinti beszerzési eljárás lefolytatása alól mentesített szerződések tárgyát és becslött értékét.”

**17. Az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet módosítása**

**59. §**

Az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet 79. §-a a következő (3) bekezdéssel egészül ki:

„(3) Ha a kormányzati hitelesítés-szolgáltatást állami költségvetési szerv nyújtja, a közfeladat ellátása céljából nyújtott bizalmi szolgáltatások tekintetében nem vonatkoznak rá a bizalmi szolgáltatókra irányadó pénzügyi követelmények és nem köteles felelősségbiztosítást kötni.”

**60. §**

Az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet a következő VIII/A. Fejezettel egészül ki:

**„VIII/A. KÉP-, HANG, KÉP- ÉS HANGFELVÉTEL KÖZPONTI TÁROLÁSÁRA  
VONATKOZÓ SZABÁLYOK**

154/B. § A Kormány az E-ügyintézési tv. szerinti kép-, hang, kép- és hangfelvételek központi tárolására tárhelyszolgáltatóként a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t jelöli ki.”

## **18. Záró rendelkezések**

### **61. §**

- (1) Ez a rendelet – a (2)-(4) bekezdésben meghatározott kivétellel – a kihirdetését követő napon lép hatályba.
- (2) A 3-33. §, 39-56. §, 58-59. § 2019. január 1-jén lép hatályba.
- (3) Az 1-2. § 2019. április 1-jén lép hatályba.
- (4) Az 60. § a kihirdetést követő hatodik hónap első napján lép hatályba.

1. melléklet a .../2018. (... ..) Korm. rendelethez

„1. melléklet a 187/2015. (VII. 13.) Korm. rendelethez

	A	B	C
1.	A jogszabálysértés megnevezése	A bírság legkisebb mértéke (Ft)	A bírság legnagyobb mértéke (Ft)
2.	regisztráció elmulasztása	50 000	100 000
3.	adatváltozás bejelentésének elmulasztása	50 000	500 000
4.	kockázatelemzés készítésének elmulasztása	200 000	500 000
5.	kockázatokkal arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása	300 000	5 000 000
6.	kockázatelemzés és a szükséges biztonsági intézkedések biztonsági eseményt követő haladéktalan, egyéb esetben évente dokumentált felülvizsgálatának elmulasztása, a felülvizsgálat során feltárt hiányosságok alapján a szükséges módosítások végrehajtásának elmulasztása	200 000	2 000 000
7.	biztonsági esemény bejelentésének elmulasztása	300 000	5 000 000
8.	hatóság végleges, végrehajtandó határozatában foglalt kötelezésének nem teljesítése	400 000	5 000 000

”