270/2018. (XII. 20.) Korm. rendelet

az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről

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

1. Hatály

1. § (1) E rendeletet kell alkalmazni
a) az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényben (a továbbiakban: Ekertv.) meghatározott bejelentés-köteles szolgáltatást nyújtó szolgáltatókra (a továbbiakban: bejelentés-köteles szolgáltató), amelyek a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény alapján nem tartoznak a mikro- és kisvállalkozások körébe, valamint
b) az Ekertv. szerinti közvetítő szolgáltatókra.
(2) E rendelet nem alkalmazható arra a bejelentés-köteles szolgáltatóra, amely kijelölt európai vagy nemzeti létfontosságú rendszerelem.

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.
(2) A hatóság az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) szerinti biztonsági események (a továbbiakban: biztonsági esemény) 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 rendvédelmi szervekkel,
bc) az Európai Unió más tagállamainak illetékes ágazati hatóságaival,
bd) a Nemzeti Adatvédelmi és Információszabadság Hatósággal,
be) az Európai Unióban nem letelepedett, Magyarországon belül szolgáltatásait kínáló bejelentés-köteles szolgáltatást nyújtók által kinevezett képviselőkkel;

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

d) szükség szerint kötelezi a szolgáltatást nyújtókat arra, hogy

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

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

e) a nyilvánosságot szükség szerint tájékoztatja az egyes biztonsági eseményekről;

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

g) hatósági ellenőrzést végez a bejelentés-köteles szolgáltatást nyújtók kötelezettségeinek teljesítése vonatkozásában;

h) az Ibtv. 19. § (1) bekezdése szerinti, az eseménykezelő központ feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló kormányrendeletben kijelölt 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 hatóságával a hatóság együttműködik.

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

a) gazdasági társaság elnevezését,

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, valamint a gazdasági társaság európai vagy nemzeti létfontosságú rendszerelemmé történő kijelöléséről szóló - a hatóság részére benyújtott - bejelentése alapján, a bejelentést követő nyolc napon belül. A gazdasági társaság az európai vagy nemzeti létfontosságú rendszerelemmé kijelölő határozat véglegessé válásától számított nyolc napon belül köteles bejelentését a hatóság részére benyújtani.

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

(4) A hatóság hatósági eljárást indít, amennyiben adatokat tárnak elé arra vonatkozóan, hogy valamely bejelentés-köteles szolgáltató nem teljesíti a jogszabályban meghatározott információbiztonsági követelményeket. Ilyen adatokat azon másik tagállam illetékes hatósága is benyújthat, amely tagállamban sor kerül az adott szolgáltatás nyújtására.

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

a) szükség esetén tájékoztatja az eseménykezelő központot, egyéb érintett szervezeteket,

b) alapvető szolgáltatásokat nyújtó szereplő érintettsége esetén tájékoztatja a kijelölő 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 (EU) 2018/151 bizottsági végrehajtási rendeletben [a továbbiakban: (EU) 2018/151 bizottsági végrehajtási rendelet] foglalt biztonsági elemek bejelentés-köteles szolgáltató általi teljesítését.

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

(9) Az ellenőrzésről az előzetes értesítés mellőzhető, ha

a) az Ibtv. szerinti súlyos biztonsági esemény történt,

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

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

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

(11) A hatóság az eljárása során jogosult figyelembe venni a független, képesített ellenőr által készített ellenőrzés eredményét, 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. § 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 közétett formában a 3. § (1) bekezdésében 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 3. § (1) bekezdésében meghatározott adatokat az (1) bekezdésben megjelölt formában benyújtani a hatóságnak.

(3) A bejelentés-köteles szolgáltatást nyújtó a 3. § (1) bekezdésében 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 az (EU) 2018/151 bizottsági végrehajtási rendeletben meghatározott paramétereket.

(3) 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.

(4) 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.

(5) 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.

(6) 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 a 4. §-ban és az 5. §-ban meghatározott követelmények teljesülését;
c) vizsgálja a bejelentés-köteles szolgáltatást nyújtó biztonsági intézkedéseinek megfelelőségét;
d) a vizsgálat során jogosult a 3. § szerinti cselekményeket elvégezni;
e) a vizsgálat eredményeként hatósági döntést hoz, amelynek tartalma legalább:
ea) a biztonsági esemény bekövetkezése 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, ha 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 a közérdeket szolgálja.

5. Jogkövetkezmények alkalmazása

7. § (1) A hatóság - határidő tűzése 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 jogszabálysértés esetén, az 1. mellékletben rögzített mértékben bírságot szabhat ki.
8. § Ha a közvetítő szolgáltató nem teljesíti az eseménykezelő központ feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló kormányrendeletben meghatározott együttműködési kötelezettségét, a hatóság az eseménykezelő központ értesítése alapján - 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 8 napon belül kell megfizetni (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, valamint 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. Záró rendelkezések

11. § (1) Ez a rendelet - a (2) bekezdésben meghatározott kivétellel - 2019. január 1-jén lép hatályba.

(2) A 2. § (2) bekezdés *h)* pontja, a 7. § (3) bekezdése, a 8-10. §, valamint az 1. melléklet az e rendelet kihirdetését követő 16. napon lép hatályba.

12. § (1) Az e rendeletben foglaltakat a rendelet hatálybalépésekor folyamatban lévő ügyekre is alkalmazni kell.

(2) A BM Országos Katasztrófavédelmi Főigazgatóság 2019. január 15-ig köteles a Nemzetbiztonsági Szakszolgálatnak átadni a bejelentés-köteles szolgáltatást nyújtókról szóló 410/2017. (XII. 15.) Korm. rendelettel kapcsolatos adatokat és a folyamatban lévő eljárásokat.

13. § (1) Ez a rendelet a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

(2) Ez a rendelet 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 (EU) 2018/151 bizottsági végrehajtási rendelet végrehajtásához szükséges rendelkezéseket állapít meg.

14. §[1]

1. melléklet a 270/2018. (XII. 20.) Korm. rendelethez

Az egyes jogszabálysértések esetében kiszabható bírság mértéke

	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

1 *Hatályon kívül helyezve: 2010. évi CXXX. törvény 12. § alapján. Hatálytalan: 2019. I. 2-től.*

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

TARTALOMJEGYZÉK

270/2018. (XII. 20.) Korm. rendelet ---- 1
az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről ---- 1
1. Hatály ---- 1
2. A hatóság hatásköre és feladatai ---- 1
3. A bejelentés-köteles szolgáltatást nyújtók elektronikus és információs rendszereinek biztonságára vonatkozó alapvető követelmények ---- 4
4. A jelentős biztonsági eseményekkel és azok bejelentésével összefüggő szabályok ---- 4
5. Jogkövetkezmények alkalmazása ---- 5
6. Záró rendelkezések ---- 6
1. melléklet a 270/2018. (XII. 20.) Korm. rendelethez ---- 6
Az egyes jogszabálysértések esetében kiszabható bírság mértéke ---- 6