



Az Európai Unió
Tanácsa

Brüsszel, 2021. január 25.
(OR. en)

5533/21

Intézményközi referenciaszám:
2020/0307(NLE)

SCH-EVAL 10
DATAPROTECT 13
COMIX 41

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Címzett:	a delegációk
Előző dok. sz.:	14247/20
Tárgy:	A Tanács végrehajtási határozata a schengeni vívmányok Magyarország általi alkalmazásának 2019. évi értékelése során az adattvédelem terén feltárt hiányosságok kiküszöbölésére vonatkozó ajánlásról

Mellékelten továbbítjuk a delegációknak a schengeni vívmányok Magyarország általi alkalmazásának 2019. évi értékelése során az adattvédelem terén feltárt hiányosságok kiküszöbölésére vonatkozó ajánlásról szóló tanácsi végrehajtási határozatot, amely 2021. január 21-én írásbeli eljárás keretében elfogadásra került.

A 2013. október 7-i 1053/2013/EU tanácsi rendelet 15. cikkének (3) bekezdésével összhangban ezt az ajánlást továbbítjuk az Európai Parlamentnek és a nemzeti parlamenteknek.

A Tanács végrehajtási határozata

a schengeni vívmányok Magyarország általi alkalmazásának 2019. évi értékelése során az adatvédelem terén feltárt hiányosságok kiküszöbölésére vonatkozó

AJÁNLÁSRÓL

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a schengeni vívmányok alkalmazását ellenőrző értékelési és monitoringmechanizmus létrehozásáról és a végrehajtó bizottságnak a Schengent Értékelő és Végrehajtását Felügyelő Állandó Bizottság létrehozásáról szóló 1998. szeptember 16-i határozatának hatályon kívül helyezéséről szóló, 2013. október 7-i 1053/2013/EU tanácsi rendeletre¹ és különösen annak 15. cikkére,

tekintettel az Európai Bizottság javaslatára,

mivel:

- (1) E határozat célja, hogy Magyarország számára korrekciós intézkedéseket ajánljon a 2019. évi schengeni értékelés során az adatvédelem terén feltárt hiányosságok kiküszöbölésére. Az értékelést követően a Bizottság a C(2020)8170 végrehajtási határozattal elfogadta a megállapításokat és értékeléseket tartalmazó jelentést, amely felsorolja az értékelés során azonosított bevált módszereket és hiányosságokat.

¹ HL L 295., 2013.11.6., 27. o.

- (2) Bevált módszereknek tekinthetők többek között a következők: a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) költségvetése folyamatosan nőtt; a SIRENE-iroda eleget tett az előző, 2012. évi schengeni adatvédelmi értékelés ajánlásainak, és most utal az érintettek számára biztosított azon lehetőségre, hogy panaszt nyújtsanak be az NAIH-hoz; a Külgazdasági és Külügyminisztérium utal a bírósági jogorvoslat lehetőségére is; a NAIH honlapján közzétett információk átfogóak, hasznosak és hozzáférhetők, könnyen elérhetők és megfogalmazásuk egyértelmű; a Külgazdasági és Külügyminisztérium erőfeszítéseket tett az információbiztonság különböző aspektusainak kezelésére és hivatalossá tételére; a Külgazdasági és Külügyminisztérium szilárd és átfogó biztonsági tervvel rendelkezik, továbbá az érintetteknek a Schengeni Információs Rendszer második generációjával (SIS II) kapcsolatos jogai gyakorlására szolgáló formanyomtatványok több nyelven (magyarul, angolul, németül, franciául és oroszul) elérhetők.
- (3) A végrehajtás tekintetében egyik ajánlás sem élvez elsőbbséget.
- (4) Ezt a határozatot továbbítani kell az Európai Parlamentnek és a tagállamok parlamentjeinek. Az 1053/2013/EU rendelet 16. cikkének (8) bekezdése értelmében Magyarországnak a határozat elfogadásától számított hat hónapon belül be kell nyújtania a Bizottságnak a (lehetséges) fejlesztésekről készített értékelését és a szükséges intézkedések leírását,

AJÁNlja, HOgy:

Magyarország

Adatvédelmi hatóság (NAIH)

1. biztosítsa, hogy a SIS II-re vonatkozó jogszabályoknak való megfelelés felügyelete során a NAIH rendszeresen ellenőrizze a SIS II figyelmeztető jelzéseit is;
2. biztosítsa, hogy a NAIH nyomon kövesse a SIS II ellenőrzései, illetve a korábbi felügyeleti intézkedések auditjai keretében megfogalmazott megállapításokat és ajánlásokat, és ezeket a 2019. évi ellenőrzési tervekben is vegye figyelembe;
3. biztosítsa, hogy a NAIH átfogóan nyomon kövesse a Vízüminformációs Rendszerre (VIS) vonatkozó felügyeleti tevékenység keretében megfogalmazott ajánlások gyakorlati végrehajtását;

4. biztosítsa, hogy a NAIH VIS-re vonatkozó felügyeleti tevékenysége kiterjedjen a nemzeti vízumrendszer valamennyi adatvédelmi vonatkozására, beleértve a külső szolgáltatók általi adatkezelést is;

Az érintettek jogai

5. terjessze ki a 15/2013. (I. 28.) Korm. rendelet 9. mellékletének hatályát (amely melléklet külön formanyomtatványt határoz meg az érintettek hozzáférési jogainak gyakorlásához), hogy az érintettek egyéb – például a helyesbítésre és a törlésre vonatkozó – jogainak gyakorlásához szükséges formanyomtatványok is rendelkezésre álljanak;
6. biztosítsa, hogy a magyar hatóságok (Országos Idegenrendészeti Főigazgatóság – OIF) tisztázzák az érintettek kérelmeinek értékelésével kapcsolatos eljárásaikat, különösen a helyesbítési vagy a törlési jog korlátozása esetén, és hangolják össze azokat az alkalmazandó uniós és nemzeti joggal;

Vízuminformációs Rendszer

7. biztosítsa a VIS kiemelt felhasználóinak kielégítő nyomon követését; ennek fényében szervezeti és műszaki intézkedésekre lehet szükség a kiemelt felhasználók nyomon követéséhez;
8. növelje az üzletmenetfolytonosság-menedzsment / a katasztrófa utáni helyreállítási terv tesztelésének gyakoriságát, különösen a Külgazdasági és Külügyminisztérium tekintetében;
9. biztosítsa, hogy a másodlagos informatikai telephely létrehozásáig az informatikai biztonsági másolatokat rövid távon ne a szerverszobának helyt adó létesítményben, hanem attól eltérő helyen tárolják;
10. növelje az informatikai eszközökhöz való hozzáférés biztonságát;
11. rendszeresen végezze el a belső fejlesztésű titkosítási rendszer biztonsági felülvizsgálatát (Külgazdasági és Külügyminisztérium);

Schengeni Információs Rendszer

12. növelje az adatközpont épületének fizikai biztonságát azáltal, hogy a második ki-, illetve belépési pontot is kamerás megfigyelés alá helyezi, továbbá fokozza a szerverszobában lévő informatikai eszközök fizikai biztonságát;
13. rendszeresen végezze el a SIS II felhasználói hozzáférést kezelő rendszerének biztonsági felülvizsgálatát;

14. biztosítsa az egységes általános információbiztonsági irányelvek/iránymutatások alkalmazását az N.SIS tekintetében (pl. jelszavakra vonatkozó szabályok stb.);
15. biztosítsa, hogy a SIRENE-iroda a nemzeti archívummal együttműködve megvizsgálja az adatmegőrzési eljárással kapcsolatos gyakoribb kiválasztási eljárás lehetőségeit;
16. növelje az üzletmenetfolytonosság-menedzsment / a katasztrófa utáni helyreállítási terv tesztelésének gyakoriságát;
17. biztosítsa, hogy a Magyar Országos Rendőr-főkapitányság (ORFK) – konkrétan az N.SIS-hivatal és a SIRENE-iroda – megoldást találjon a kiemelt felhasználók ellenőrzésére;
18. biztosítsa, hogy a SIRENE-iroda aktívabb szerepet játsszon a SIS II-be bevitt információk minőség-ellenőrzésének koordinálásában a SIRENE-kézikönyv 1.15. pontjában leírtak szerint;

A lakosság tájékoztatása

19. biztosítsa, hogy a Külgazdasági és Külügyminisztérium egyértelműen kijelölje a VIS-szel foglalkozó adatkezelő(ke)t. Az átláthatóság biztosítása, valamint az egyéni jogok gyakorlásának lehetővé tétele érdekében fontos, hogy az érintettek megfelelő tájékoztatást kapjanak az egyes adatkezelők felelősségi köréről;
20. biztosítsa, hogy az ORFK rendszeresen frissítse a SIS-re vonatkozó szakaszt tartalmazó tájékoztató angol változatát.

Kelt Brüsszelben,

a Tanács részéről

az elnök