FRANCIA KÖZTÁRSASÁG

A miniszterelnök

Rendelettervezet a felhőalapú számítástechnika piacán a stratégiai és érzékeny adatok védelméről

NOR:

Érintettek: *Államigazgatási szervek és szereplők, közérdekű társulások*

Tárgy: *…*

Hatálybalépés*: a rendelet a kihirdetését követő napon lép hatályba.*

Értesítés: *….*

Hivatkozások: *A rendelet a digitális tér biztonságossá tételéről és szabályozásáról szóló, 2024. május 21-i 2024-449. sz. törvény 31. cikkét hajtja végre. Megtekinthető a Légifrance honlapján (http://www.legifrance.gouv.fr).*

A Miniszterelnök,

a(z) XX jelentése alapján,

tekintettel az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendeletre (kiberbiztonsági jogszabály),

tekintettel a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról szóló, 2015. szeptember 9-i (EU) 2015/1535 európai parlamenti és tanácsi irányelvre,

tekintettel a védelmi törvénykönyvre és különösen annak D. 3126-2. cikkére,

tekintettel a felhasználók és a közigazgatási hatóságok közötti, valamint a közigazgatási hatóságok közötti elektronikus információcseréről szóló, 2005. december 8-i 2005-1516. sz. rendeletre és különösen annak 9. cikkére,

tekintettel a digitális köztársaságról szóló, 2016. október 7-i 2016-1321. sz. törvényre és különösen annak 16. cikkére,

tekintettel a digitális tér biztonságossá tételéről és szabályozásáról szóló, 2024. május 21-i 2024-449. sz. törvényre és különösen annak 31. cikkére,

tekintettel a Belső Biztonsági Főigazgatóság feladatairól és szervezetéről szóló, 2014. április 30-i 2014-445. sz. rendeletre,

tekintettel a biztonsági termékeknek és a bizalmi szolgáltatóknak az információs rendszerek biztonsági igényei tekintetében történő minősítéséről szóló, 2015. március 27-i 2015-350. sz. módosított rendeletre,

tekintettel az Európai Bizottságnak XXX-án/-én küldött XX. sz. értesítésre,

az Államtanáccsal (Igazgatási szekció) folytatott konzultációt követően,

az alábbiakat rendeli el:

1. cikk

A közérdekű társulásoknak a fent említett 2024. május 21-i törvény 31. cikkének I. pontjában említett listája a következőket tartalmazza:

- a „Digitális Egészségügyi Ügynökség (Agence du numérique en santé – ANS)” néven ismert közérdekű társulás;
- a „Nemzeti AIDS-kutatási Ügynökség (Agence nationale de recherches sur le sida – ANRS)” néven ismert közérdekű társulás;
- „a képzések, valamint az oktatási és tudományos csereprogramok előmozdításával foglalkozó ügynökség” (Agence de promotion des formations et des échanges éducatifs et scientifique) néven ismert közérdekű társulás;
- a „Biztonságos Adathozzáférési Központ (Centre d’accès sécurisé aux données – CASD)” közérdekű társulás;
- „A radikalizálódás megelőzésével foglalkozó erőforrásközpont” (Centre ressources prévention de la radicalisation) közérdekű társulás;
- a „Nemzeti Állatorvosi Iskola” (Ecole naionale des services vétérinaires) közérdekű társulás;
- „A nagy aktivitású zárt sugárforrásokkal foglalkozó közérdekű társulás (Groupement d'intérêt public relatif aux sources radioactives scellées de haute activité – GIP SOURCES HA)” nevű közérdekű társulás;
- „A szociális lakások iránti kereslet nyilvántartásának nemzeti rendszere (Groupement d’intérêt public Système national d’enregistrement de la demande de logement social – GIP SNE)” közérdekű társulás;
- „A szociális nyilatkozatok korszerűsítése (Groupement d’intérêt public Modernisation des Déclarations Sociales – GIP-MDS)” közérdekű társulás;
- a „Tudományos és Technológiai Megfigyelőközpont” (Observatoire des sciences et des techniques) közérdekű társulás.

2. cikk

I. – A fent említett 2024. május 21-i törvény 31. cikkének alkalmazásában a magánszolgáltatónak a következő biztonsági és adatvédelmi kritériumokat kell teljesítenie:

- az alvállalkozói láncot magában foglaló dokumentált információbiztonsági és kockázatkezelési politika;
- biztonságos humánerőforrás-gazdálkodási rendszer a szolgáltatás nyújtásában részt vevő személyzet tekintetében;
- a szolgáltatást nyújtó berendezések és az információs rendszerek biztonságos kezeléséhez szükséges eszközök és eljárások;
- fizikai, környezeti és logikai biztonsági intézkedések, például titkosítási mechanizmusok, hozzáférés-ellenőrzés és felhasználói személyazonosság-kezelés alkalmazása;
- információbiztonsági incidenskezelési eljárások és üzletmenet-folytonossági intézkedések;
- a Franciaországban hatályos jogi rendelkezések betartását biztosító intézkedések, valamint adatvédelmi intézkedések, különösen szerződésben foglalt intézkedések, amelyek a kezelt vagy tárolt adatok védelmét szolgálják a harmadik országok hatóságainak az uniós jog vagy a tagállami jog által nem engedélyezett hozzáférésével szemben, ideértve különösen a szolgáltató vállalatában birtokolt tőkerészesedésre és szavazati jogokra, valamint a szolgáltató és az esetleges alvállalkozók letelepedésére vonatkozó feltételeket.

A Francia Kiberbiztonsági Ügynökség által a fent említett 2015. március 27-i rendelet feltételei szerint kidolgozott keretrendszer megállapítja az e kritériumokra vonatkozó követelményeket. Az állami információs rendszer referenciakeretének létrehozásához és fejlesztéséhez szükséges konzultációt a Minisztériumközi Digitális Igazgatósággal együttműködve kell lefolytatni.

II. – A fent említett 2024. május 21-i törvény 31. cikkének I. pontjában meghatározott adatvédelmi és biztonsági követelmények teljesítése érdekében az érintett közigazgatási szervek olyan magánszolgáltató által nyújtott felhőszolgáltatásokat vesznek igénybe, amely a fent említett 2015. március 27-i rendelet III. fejezetében meghatározott feltételek szerint odaítélt minősítéssel rendelkezik, és megfelel az e cikk I. pontjában említett kritériumoknak, vagy legalább azonos szintű európai tanúsítvánnyal rendelkezik.

III. – Nem tartoznak e cikk hatálya alá az üzemeltetési és kommunikációs információs rendszerek, a tudományos és műszaki információs rendszerek, valamint azok az információs rendszerek, amelyek a védelmi információs és kommunikációs rendszert alkotó minősített adathordozókat vagy információkat használnak fel, igényelnek vagy tartalmaznak, valamint a védelmi törvénykönyv D. 3126-2. cikkében és a fent említett 2014. április 30-i rendelet 1. cikkében említett szolgálatok által működtetett információs és kommunikációs rendszerek.

3. cikk

I. – Ha valamely közigazgatási szerv a fent említett 2024. május 21-i törvény 31. cikkének hatálybalépésekor már megkezdett egy olyan projektet, amely megfelel a fent említett cikkben meghatározott feltételeknek, és amely olyan magánszolgáltató által nyújtott felhőszolgáltatást

vesz igénybe, amely nem teljesíti az e rendelet 2. cikkében meghatározott biztonsági és adatvédelmi kritériumokat, a miniszterelnök rendeletében meghatározott eljárásoknak megfelelően eltérést kérhet az ugyanezen cikkben meghatározott kötelezettségek alól.

Ez az eltérés nem haladhatja meg a 18 hónapot, amennyiben Franciaországban elérhető az e cikk II. pontja szerinti, felhőszolgáltatásokra vonatkozó elfogadható ajánlat. Amennyiben az eltérés iránti kérelem időpontjában Franciaországban nem érhető el elfogadható felhőalapú ajánlat, az eltérés nem haladhatja meg az egy évet egy lehetséges új kérelem előtt.

Ezt az eltérést a projektért felelős miniszter indokolással ellátott és a miniszterelnök által jóváhagyott határozatával kell engedélyezni.

A határozatot a nyilvánosság és a közigazgatás közötti kapcsolatokról szóló törvénykönyv III. könyvében meghatározott feltételek szerint kell közzétenni.

II. – A felhőszolgáltatásokra vonatkozó ajánlatnak a fent említett 2024. május 21-i törvény 31. cikkének III. pontja szerinti elfogadhatóságát a következő kritériumok alapján kell értékelni:

- az a funkcionális igény, amelyet az ajánlat képes kielégíteni, figyelembe véve az érintett közigazgatási szerv feladatait;
- a pénzügyi feltételek;
- az ajánlattevő által kezelt adatok biztonságának és védelmének működési és technikai feltételei az e rendelet 2. cikkében meghatározott követelményekre tekintettel;
- a szerződés megszűnésének feltételei és az adatvisszaállítási garanciák;
- a fent említett 2016. október 7-i törvény 16. cikke szerinti ellenőrzési, fenntarthatósági és függetlenségi feltételek.

Kelt:

A miniszterelnök nevében: