REPUBLIKEN FRANKRIKE

Premiärministern

Utkast till dekret om skydd av strategiska och känsliga uppgifter på marknaden för molntjänster

NOR:

Målgrupp: *Statliga förvaltningar och operatörer, offentliga intressegrupper*

Ämne: *…*

Ikraftträdande: *texten träder i kraft dagen efter det att den har offentliggjorts.*

Anmärkning: *….*

Referenser: *Genom dekretet genomförs artikel 31 i lag nr 2024-449 av den 21 maj 2024 om säkerställande och reglering av det digitala området. Den kan ses på Légifrances webbplats (http://www.legifrance.gouv.fr).*

Premiärministern utfärdar detta dekret,

om rapporten från XX,

med beaktande av Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om ENISA (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten),

med beaktande av Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster,

med beaktande av försvarslagen, särskilt artikel D. 3126-2,

med beaktande av förordning nr. 2005–1516 av den 8 december 2005 om elektroniskt utbyte mellan användare och administrativa myndigheter samt mellan administrativa myndigheter, särskilt artikel 9,

med beaktande av lag nr 2016-1321 av den 7 oktober 2016 för en digital republik, särskilt artikel 16,

med beaktande av lag nr 2024-449 av den 21 maj 2024 om säkerställande och reglering av det digitala området, särskilt artikel 31 däri,

med beaktande av dekret nr 2014-445 av den 30 april 2014 om uppgifter och organisation för generaldirektoratet för inre säkerhet,

med beaktande av dekret nr 2015-350 av den 27 mars 2015, i dess ändrade lydelse, om kvalificering av säkerhetsprodukter och tillhandahållare av betrodda tjänster för informationssystemens säkerhetsbehov,

med beaktande av anmälan nr XX som skickats till Europeiska kommissionen den XXX,

efter samråd med statsrådet (förvaltningsavdelningen).

Härigenom föreskrivs följande.

Artikel 1

Den förteckning över de offentliga intressegrupperingar som avses i artikel 31(I) i ovannämnda lag av den 21 maj 2024 omfattar följande:

- Den offentliga intressegrupperingen med namnet *Agence du Numérique en Santé - ANS* (den franska e-hälsomyndigheten).
- Den offentliga intressegrupperingen med namnet *Agence nationale de recherches sur le sida (ANRS)* (Den nationella byrån för forskning om AIDS).
- Den offentliga intressegrupperingen med namnet *Agence de promotion des formations et des échanges éducatifs et scientifiques* (Byrån för främjande av utbildning och vetenskapligt utbyte.
- Den offentliga intressegrupperingen *Centre d'accès sécurisé aux données (CASD)* (Centrumet för säker dataåtkomst).
- Den offentliga intressegrupperingen *Centre ressources prévention de la radicalisation* (Resurscentrum för förebyggande av radikalisering).
- Den offentliga intressegrupperingen *Ecole nationale des services vétérinaires* (Nationella veterinärskolan).
- Den offentliga intressegrupperingen *Groupement d'intérêt public relatif aux sources radioactives scellées de haute activité (GIP SOURCES HA)* (Den offentliga intressegrupperingen om förseglade högaktiva radioaktiva källor).
- Den offentliga intressegrupperingen *Système national d'enregistrement de la demande de logement social (GIP SNE)* (Nationellt system för registrering av efterfrågan på sociala bostäder).
- Den offentliga intressegrupperingen *Modernisation des déclarations sociales (GIP-MDS)* (Modernisering av sociala deklarationer).
- Den offentliga intressegrupperingen *Observatoire des sciences et des techniques* (Observatoriet för vetenskap och teknik).

Artikel 2

I - För tillämpningen av artikel 31 i ovannämnda lag av den 21 maj 2024 måste den privata tjänsteleverantören genomföra följande säkerhets- och dataskyddskriterier:

- En dokumenterad policy för informationssäkerhet och riskhantering som omfattar underleverantörskedjan.
- Ett säkert personalförvaltningssystem för personal som deltar i tillhandahållandet av tjänsten.
- Verktyg och förfaranden för säker hantering av utrustning som implementerar tjänste- och informationssystemen.
- Fysiska, miljömässiga och logiska säkerhetsåtgärder, såsom användning av krypteringsmekanismer, åtkomstkontroll och hantering av användaridentitet.
- Förfaranden för hantering av informationssäkerhetsincidenter och åtgärder för kontinuitet i verksamheten.
- Åtgärder för efterlevnad av gällande lagstiftning i Frankrike och dataskyddsåtgärder, särskilt avtalsmässiga sådana, för behandlade eller lagrade uppgifter mot åtkomst av offentliga myndigheter i tredjeländer som inte är tillåtna enligt EU-lagstiftningen eller lagstiftningen i en medlemsstat, inbegripet i synnerhet villkor för kapitalinnehav och rösträtt i tjänsteleverantörens företag samt tjänsteleverantörens och eventuella underleverantörers etablering.

En ram som utvecklats av den franska cybersäkerhetsbyrån enligt villkoren i ovannämnda dekret av den 27 mars 2015 fastställer de krav som hänför sig till dessa kriterier. Det samråd som krävs för att skapa och utveckla denna referensram för det statliga informationssystemet ska genomföras i samarbete med det interministeriella digitala direktoratet.

II - För att uppfylla dataskydds- och säkerhetskraven i artikel 31.I i ovannämnda lag av den 21 maj 2024 ska de berörda förvaltningarna ha tillgång till molntjänster som tillhandahålls av en kvalificerad privat tjänsteleverantör, som tilldelas på de villkor som anges i kapitel III i ovannämnda dekret av den 27 mars 2015 och som uppfyller de kriterier som avses i punkt I i denna artikel, eller en europeisk certifiering på minst motsvarande nivå.

III - Informationssystem för drift och kommunikation, vetenskapliga och tekniska informationssystem, och informationssystem som inbegriper, kräver eller innehåller sekretessbelagda medier eller sekretessbelagd information som omfattar försvarsinformations- och kommunikationssystemet samt de informations- och kommunikationssystem som drivs av de tjänster som avses i artikel D. 3126-2 i försvarslagen och artikel 1 i ovannämnda dekret av den 30 april 2014 är undantagna från denna artikels tillämpningsområde.

Artikel 3

I - Om en förvaltning redan den dag då artikel 31 i ovannämnda lag av den 21 maj 2024 träder i kraft har inlett ett projekt som uppfyller villkoren i nämnda artikel och som använder en molntjänst som tillhandahålls av en privat tjänsteleverantör som inte uppfyller de säkerhets- och dataskyddskriterier som fastställs i artikel 2 i detta dekret, får den, i enlighet med de förfaranden som fastställs genom premiärministerns beslut, begära ett undantag från de skyldigheter som fastställs i samma artikel.

Detta undantag får inte överstiga 18 månader om det finns ett godtagbart erbjudande om molntjänster, i den mening som avses i punkt II i denna artikel, tillgängligt i Frankrike. Om det inte finns något godtagbart molnerbjudande tillgängligt i Frankrike vid tidpunkten för begäran om undantag, får undantaget inte överskrida ett år före en eventuell ny begäran.

Detta undantag beviljas genom ett motiverat beslut av den minister som ansvarar för projektet och valideras av premiärministern.

Den ska offentliggöras på de villkor som anges i avdelning III i PR-lagen.

II – Bedömningen av huruvida ett erbjudande om molntjänster är godtagbart, i den mening som avses i artikel 31(III) i lagen av den 21 maj 2024, grundar sig på följande kriterier:

- Det funktionella behov som anbudet kan tillgodose, med beaktande av den berörda förvaltningens uppgifter.
- De finansiella villkoren.
- De operativa och tekniska villkoren för datasäkerhet och dataskydd för de uppgifter som behandlas av leverantören av erbjudandet i enlighet med kraven i artikel 2 i detta dekret.
- Villkoren för när avtalet upphör att gälla och reversibilitetsgarantier.
- Villkoren för kontroll, hållbarhet och oberoende i den mening som avses i artikel 16 i ovannämnda lag av den 7 oktober 2016.

Utfärdat den

Av premiärministern: