FRANSE REPUBLIEK

De minister-president

Ontwerpbesluit inzake de bescherming van strategische en gevoelige gegevens op de markt voor cloud computing

NOR:

Doelgroep: *Overheidsdiensten en exploitanten, belangengroepen*

Betreft: …

Inwerkingtreding: *het besluit treedt in werking op de dag na de bekendmaking ervan.*

Opmerking: ….

Referenties: *Het besluit geeft uitvoering aan artikel 31 van wet nr. 2024-449 van 21 mei 2024 inzake de beveiliging en regulering van de digitale ruimte. Het kan worden geraadpleegd op de website van Légifrance (http://www.legifrance.gouv.fr).*

De Minister-president,

Over het verslag van XX,

Gezien Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening);

Gezien Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij;

Gezien de defensiewet, in het bijzonder artikel D. 3126-2;

Gezien besluit 2005-1516 van 8 december 2005 inzake elektronische uitwisselingen tussen gebruikers en administratieve autoriteiten en tussen administratieve autoriteiten, en met name artikel 9 daarvan;

Gezien wet 2016-1321 van 7 oktober 2016 voor een Digitale Republiek, in het bijzonder artikel 16 daarvan;

Gezien wet 2024-449 van 21 mei 2024 inzake de beveiliging en regulering van de digitale ruimte, met name artikel 31 daarvan,

Gezien besluit 2014-445 van 30 april 2014 betreffende de taken en de organisatie van het directoraat-generaal voor Binnenlandse Veiligheid;

Gezien besluit 2015-350 van 27 maart 2015, zoals gewijzigd, betreffende de kwalificatie van beveiligingsproducten en aanbieders van vertrouwensdiensten voor de beveiligingsbehoeften van informatiesystemen;

Gezien kennisgeving XX toegezonden aan de Europese Commissie op XXX;

Na raadpleging van de Raad van State (Afdeling Administratie),

Beschikt:

Artikel 1

De in artikel 31, punt I, van voornoemde wet van 21 mei 2024, bedoelde lijst van organisaties van openbaar belang omvat:

- de belangengroep die bekendstaat als "Agentschap voor Digitale Gezondheid (ANS)";
- de belangengroep die bekendstaat als "Nationaal Agentschap voor AIDS Onderzoek (ANRS)";
- de belangengroep, die bekendstaat als "Agentschap voor de Bevordering van Onderwijs- en Wetenschappelijke Opleiding en Uitwisseling";
- de belangengroep "Centrum voor toegang tot veilige gegevens (CASD)";
- de belangengroep "Centrum voor middelen ter voorkoming van radicalisering";
- de belangengroep "Nationale diergeneeskundige school";
- de belangengroep "Belangengroep voor verzegelde radioactieve bronnen met hoge activiteit" (GIP SOURCES HA)";
- de belangengroep "Nationaal systeem voor de registratie van de vraag naar sociale huisvesting (GIP SNE)";
- de belangengroep "Modernisering van sociale verklaringen (GIP-MDS)";
- de belangengroep "Waarnemingspost wetenschap en technologie".

Artikel 2

I - Voor de toepassing van artikel 31 van voornoemde wet van 21 mei 2024 moet de particuliere dienstverlener de volgende beveiligings- en gegevensbeschermingscriteria toepassen:

- een gedocumenteerd beleid inzake informatiebeveiliging en risicobeheer waarin de onderaannemingsketen is opgenomen;
- een beveiligd systeem voor personeelsbeheer voor het personeel dat betrokken is bij de verlening van de dienst;
- instrumenten en procedures voor het veilig beheer van apparatuur voor de implementatie van de diensten- en informatiesystemen;
- fysieke, ecologische en logische beveiligingsmaatregelen, zoals het gebruik van versleutelingsmechanismen, toegangscontrole en gebruikersidentiteitsbeheer;
- procedures voor het beheer van informatiebeveiligingsincidenten en bedrijfscontinuïteitsmaatregelen;
- maatregelen voor de naleving van de in Frankrijk geldende wettelijke bepalingen en maatregelen voor bescherming van gegevens, met name contractuele, verwerkte of opgeslagen gegevens, tegen elke toegang door overheidsinstanties van derde landen die niet zijn toegestaan op grond van het recht van de Europese Unie of het recht van een lidstaat, met inbegrip van met name de voorwaarden voor het beheren van kapitaal en stemrechten in de onderneming van de dienstverlener en de vestiging van de dienstverlener en eventuele onderaannemers.

Een kader, ontwikkeld door het Frans Agentschap voor cyberbeveiliging onder de voorwaarden van voornoemd besluit van 27 maart 2015, stelt de eisen met betrekking tot deze criteria vast. De raadpleging die nodig is voor de totstandbrenging en ontwikkeling van dit referentiekader voor het staatsinformatiesysteem wordt uitgevoerd in samenwerking met het Interministerieel Digitaal Directoraat.

II - Om te voldoen aan de vereisten inzake gegevensbescherming en -beveiliging van artikel 31, punt I, van voornoemde wet van 21 mei 2024, kunnen de betrokken overheidsdiensten een beroep doen op diensten voor cloud computing die worden verleend door een gekwalificeerde particuliere dienstverlener, gegund onder de voorwaarden van hoofdstuk III van voornoemd besluit van 27 maart 2015, en die voldoen aan de in punt I van dit artikel bedoelde criteria, of van een Europese certificering van ten minste een gelijkwaardig niveau.

III - Operationele en communicatie-informatiesystemen, wetenschappelijke en technische informatiesystemen, en informatiesystemen die geclassificeerde media of informatie omvatten, vereisen of bevatten en de defensie-informatie- en -communicatiesysteem omvatten, alsmede de informatie- en communicatiesystemen die worden geëxploiteerd door de diensten bedoeld in artikel D. 3126-2 van de defensiewet en artikel 1 van voornoemd besluit van 30 april 2014, zijn uitgesloten van het toepassingsgebied van dit artikel.

Artikel 3

Wanneer een overheidsinstantie op de datum van inwerkingtreding van artikel 31 van voornoemde wet van 21 mei 2024, reeds een project heeft geïnitieerd dat voldoet aan de voorwaarden van voornoemd artikel en gebruikmaakt van een dienst voor cloud computing die wordt aangeboden door een particuliere dienstverlener die niet voldoet aan de beveiligings- en gegevensbeschermingscriteria van artikel 2 van dit besluit, kan zij overeenkomstig de bij besluit van de minister-president vastgestelde procedures verzoeken om een ontheffing van de in hetzelfde artikel vastgestelde verplichtingen.

Deze ontheffing mag niet langer duren dan 18 maanden wanneer er in Frankrijk een aanvaardbaar aanbod van diensten voor cloud computing in de zin van punt II van dit artikel beschikbaar is. Indien er in Frankrijk op de datum van het verzoek om ontheffing geen

aanvaardbaar cloudaanbod beschikbaar is, mag de ontheffing niet langer duren dan één jaar voordat een mogelijk nieuw verzoek wordt ingediend.

Deze ontheffing wordt toegestaan bij een met redenen omkleed besluit van de minister die verantwoordelijk is voor het project en wordt gevalideerd door de minister-president.

Zij wordt openbaar gemaakt onder de voorwaarden die zijn vastgesteld in Boek III van de public-relationswet.

II – De beoordeling van de aanvaardbaarheid van een aanbod van diensten voor cloud computing in de zin van artikel 31, punt III, van voormelde wet van 21 mei 2024, is gebaseerd op de volgende criteria:

- de functionele behoefte waaraan het aanbod kan voldoen, rekening houdend met de taken van de betrokken administratie;
- de financiële voorwaarden;
- de operationele en technische voorwaarden inzake gegevensbeveiliging en -bescherming voor de gegevens die door de aanbieder van het aanbod worden verwerkt overeenkomstig de vereisten van artikel 2 van dit besluit;
- de voorwaarden voor het einde van het contract en de omkeerbaarheidsgaranties;
- de controle-, duurzaamheids- en onafhankelijkheidsvoorwaarden in de zin van artikel 16 van voornoemde wet van 7 oktober 2016.

Gedaan op.

Door de Minister-president: