RÉPUBLIQUE FRANÇAISE

Premier ministre

Projet de décret relatif à la protection des données stratégiques et sensibles sur le marché de l'informatique en nuage

NOR :

Publics concernés : *administrations et opérateurs de l'Etat, groupements d'intérêt public*

Objet : *…*

Entrée en vigueur : *le décret entre en vigueur le lendemain de sa publication.*

Notice : *….*

Références : *Le décret est pris pour l'application de l'article 31 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. Il peut être consulté sur le site Légifrance (http://www.legifrance.gouv.fr).*

Le Premier ministre,

Sur le rapport de XX,

Vu le règlement n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 ;

Vu la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la défense, notamment son article D. 3126-2 ;

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment son article 9 ;

Vu la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, notamment son article 16 ;

Vu la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, notamment son article 31 ;

Vu le décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieur ;

Vu le décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information ;

Vu la notification n° XX adressée le XXX à la Commission européenne ;

Le Conseil d'Etat (section de l'administration) entendu,

Décrète :

Article 1er

La liste des groupements d'intérêt public mentionnée au I de l'article 31 de la loi du 21 mai 2024 susvisée comprend :

- Le groupement d'intérêt public dénommé « Agence du numérique en santé (ANS) » ;
- Le groupement d'intérêt public dénommé « Agence nationale de recherches sur le sida (ANRS) » ;
- Le groupement d'intérêt public dénommé « Agence de promotion des formations et des échanges éducatifs et scientifiques » ;
- Le groupement d'intérêt public « Centre d'accès sécurisé aux données (CASD) » ;
- Le groupement d'intérêt public « Centre ressources prévention de la radicalisation » ;
- Le groupement d'intérêt public « Ecole nationale des services vétérinaires » ;
- Le groupement d'intérêt public « Groupement d'intérêt public relatif aux sources radioactives scellées de haute activité (GIP SOURCES HA) » ;
- Le groupement d'intérêt public « Système national d'enregistrement de la demande de logement social (GIP SNE) » ;
- Le groupement d'intérêt public « Modernisation des déclarations sociales (GIP-MDS) » ;
- Le groupement d'intérêt public « Observatoire des sciences et des techniques ».

Article 2

I - Pour l’application de l’article 31 de la loi du 21 mai 2024 susvisée, le prestataire privé doit mettre en œuvre les critères de sécurité et de protection des données suivants :

- une politique de sécurité de l’information et de gestion du risque documentée intégrant la chaîne de sous-traitance ;
- un dispositif sécurisé en matière de gestion des ressources humaines pour les personnels impliqués dans la fourniture du service ;
- des outils et procédures de gestion sécurisée des équipements mettant en œuvre le service et des systèmes d’information ;
- des mesures de sécurité physique, environnementale et logique telles que l’utilisation de mécanismes de chiffrement, de contrôle des accès et de gestion des identités des utilisateurs ;
- des procédures et des mesures de gestion des incidents liés à la sécurité de l’information, et à la continuité de l’activité ;
- des mesures de conformité aux dispositions légales en vigueur en France et des mesures, notamment contractuelles, de protection des données traitées ou stockées contre tout accès par des autorités publiques d'Etats tiers non autorisé par le droit de l'Union européenne ou le droit d'un Etat membre comprenant en particulier des conditions de détention de capital et des droits de vote dans la société du prestataire et d’établissement du prestataire et de ses éventuels sous-traitants.

Un référentiel, élaboré par l’Agence nationale de la sécurité des systèmes d’information dans les conditions du décret du 27 mars 2015 susvisé, détermine les exigences relatives à ces critères. La concertation nécessaire à la constitution et à l’évolution de ce référentiel pour le système d’information de l’Etat est conduite en liaison avec la direction interministérielle du numérique.

II - Afin de satisfaire aux exigences de protection et de sécurité des données prévues par le I de l’article 31 de la loi du 21 mai 2024 susvisé, les administrations concernées recourent aux services d’informatique en nuage fournis par un prestataire privé ayant fait l’objet d’une qualification, attribuée dans les conditions prévues au chapitre III du décret du 27 mars 2015 susvisé et répondant aux critères mentionnées au I du présent article, ou d’une certification européenne d’un niveau au moins équivalent.

III - Sont exclus du champ d’application du présent article les systèmes d’information opérationnels et de communication, les systèmes d’information scientifiques et techniques et les systèmes d’information qui font intervenir, nécessitent ou comportent des supports ou informations classifiés composant le système d’information et de communication de la défense ainsi que les systèmes d’information et de communication opérés par les services mentionnés à l’article D. 3126-2 du code de la défense et à l’article 1er du décret du 30 avril 2014 susvisé.

Article 3

I - Lorsqu’une administration a déjà engagé, à la date d’entrée en vigueur de l’article 31 de la loi du 21 mai 2024 susvisé, un projet remplissant les conditions définies à l’article précité et recourant à un service d’informatique en nuage fourni par un prestataire privé ne mettant pas en œuvre les critères de sécurité et de protection des données définis à l’article 2 du présent décret, elle peut demander, selon des modalités fixées par arrêté du Premier ministre, une dérogation aux obligations prévues par le même article.

Cette dérogation ne peut excéder dix-huit mois lorsqu'il existe une offre de services d'informatique en nuage acceptable, au sens du II du présent article, est disponible en France. Lorsqu'il n'existe pas d'offre acceptable en nuage disponibles en France à la date de la demande de dérogation, celle-ci ne peut excéder un an avant une éventuelle nouvelle demande.

Cette dérogation est accordée par décision motivée du ministre dont le projet relève et validée par le Premier ministre.

Elle est rendue publique dans les conditions prévues par le livre III du code des relations entre le public et l'administration.

II – L'évaluation du caractère acceptable, au sens du III de l'article 31 de la loi du 21 mai 2024 susvisée, d'une offre de services d'informatique en nuage se fonde sur les critères suivants :

- le besoin fonctionnel auquel l'offre est en mesure de répondre, compte tenu des missions de l'administration concernée ;
- les conditions financières ;
- les conditions opérationnelles et techniques de sécurité et de protection des données traitées par le fournisseur de l'offre au regard des exigences définies à l'article 2 du présent décret ;
- les conditions de fin de contrat et les garanties de réversibilité ;
- les conditions de maîtrise, de pérennité et d'indépendance, au sens de l'article 16 de la loi du 7 octobre 2016 susvisée.

Fait le,

Par le Premier ministre :