CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Communication présentée en séance plénière le 28 septembre 2023

Communication sur la stratégie nationale pour l'informatique en nuage (le « *cloud* »)

Rapporteur : M. **François PELLEGRINI**

Avec le concours de :

[redacted]

Table des matières

Introduction

Le gouvernement a publié le 31 mai 2023 une circulaire actualisant la précédente circulaire du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État « *cloud* au centre », l'un des trois axes de la stratégie nationale pour le *cloud*, qui fait du *cloud* le mode d'hébergement par défaut des projets numériques de l'État.

Cette actualisation a pour objectif de préciser les conditions d'application de cette doctrine en cas de recours à une offre de *cloud* commercial « afin de mieux délimiter le périmètre des données d'une sensibilité particulière pour lesquelles le recours à une solution d'hébergement qualifiée SecNumCloud (ou disposant d'une qualification équivalente) et immunisée au droit extracommunautaire est requis ainsi que de préciser les modalités de demandes dérogation à cette règle ».

La présente communication identifie les conséquences de cette nouvelle circulaire pour la CNIL.

1. Rappel de la stratégie nationale pour l'informatique en nuage

Afin de relever les défis en matière de souveraineté et de protection de données, le Gouvernement a lancé, le 17 mai 2021, une stratégie nationale pour l'informatique en nuage (« *cloud* »).

Cette stratégie se décline en trois axes :

- Le « ***cloud* de confiance** » au travers de la qualification **SecNumCloud** de l'ANSSI (v. Annexe C : Détails de la stratégie nationale pour le cloud (axes 1 & 3)) ;
- La doctrine « ***cloud* au centre** » comme levier de la transformation numérique de l'État (v. Section 2) ;
- La stratégie **d'accélération *cloud*** via un soutien de la filière et des administrations (v. Annexe C Détails de la stratégie nationale pour le cloud (axes 1 & 3)).

2. Réécriture de la règle R9 de la doctrine « *cloud* au centre »

A. La doctrine « *cloud* au centre » comme levier de la transformation numérique de l'État

Elle a été formalisée dans **la circulaire n° 6282/SG du 5 juillet 2021** relative à la doctrine d'utilisation de l'informatique en nuage par l'État[1], puis actualisée par **la circulaire n° 6404/SG du 31 mai 2023[2].**

Les circulaires du 5 juillet 2021 et du 31 mai 2023 prévoient que « *cette doctrine s'applique **aux acteurs de l'État et aux organismes placés sous sa tutelle**, comme retenus dans le décret 2019-1088 définissant le système d'information de l'État* ».

Le décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique définit celui-ci comme étant composé de l'ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker sous forme numérique les données qui **concourent aux missions des services de l'État et des organismes placés sous sa tutelle** (article 1 du décret).

Sont exclus du champ d'application de ce décret :

- les systèmes d'information opérationnels et de communication du SI de la défense[3] ;
- les systèmes d'information scientifiques et techniques du SI de la défense[4] ;
- les services opérés par la DGSE[5] ;

[1] Circulaire n° 6282-SG du 5 juillet 2021 https://www.legifrance.gouv.fr/circulaire/id/45205
[2] Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« *cloud* au centre ») https://www.legifrance.gouv.fr/circulaire/id/45446
[3] Article 2 du décret n° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication
[4] Ibid
[5] Article D. 3126-2 du code de la défense

- les services opérés par la DGSI[6].

Avec cette doctrine, l'informatique en nuage devient dorénavant le mode d'hébergement et de production **par défaut** des **services numériques de l'État (et des organismes placés sous sa tutelle[7]), pour tout nouveau produit numérique et pour les produits connaissant une évolution substantielle[8]**.

En application de cette doctrine, les services numériques des administrations doivent être hébergés :

- sur l'un des deux *clouds* interministériels internes de l'État (« ***cloud* interne** ») ; ou
- sur les offres de cloud proposées par les industriels (« ***cloud* commercial** ») satisfaisant des critères stricts de sécurité.

En particulier, la **règle R9** (version 2021), pour l'IaaS et le PaaS, et la règle R14, pour le SaaS, prévoient que, dans le cas d'un recours à une offre de ***cloud* commercial** :

- les traitements de données à caractère personnel dans le *cloud* doivent être conformes au RGPD ;
- Les traitements de données de santé doivent être hébergés chez un prestataire certifié HDS ;
- Les traitements des données d'une « **sensibilité particulière** » doivent être opérés par **un prestataire qualifié SecNumCloud** et **être immunisés contre toute réglementation extracommunautaire**.

Dans une note interne[9] adressée aux secrétaires généraux des ministères et datée du 15 septembre 2021, la DINUM a fait savoir que la suite collaborative Microsoft 365 n'était pas conforme à la doctrine « *cloud* au centre », au titre de la règle R9.

B. Réécriture de la règle R9

[redacted]

[6] Article 1er du décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure
[7] Voir un exemple d'organismes visés par la doctrine en Annexe B
[8] Voir le courrier de Jean Castex en préambule de la circulaire du 5 juillet 2021
[9] Note interne de la DINUM concernant la conformité de Microsoft 365 à la doctrine « *cloud* au centre » https://acteurspublics.fr/upload/media/default/0001/36/acf32455f9b92bab52878ee1c8d83882684df1cc.pdf

La nouvelle rédaction, validée par la Commission européenne et publiée dans la circulaire du 31 mai 2023 (v. tableau en Annexe A : Règle R9), précise :

- les cas d'application de R9 et ;

- le périmètre des « **données d'une sensibilité particulière** », en prenant en compte les différentes exigences et exceptions découlant des traités internationaux.

En particulier la nouvelle version de la règle R9 :

- réaffirme la conformité au RGPD comme premier critère à prendre en compte lorsqu'un traitement de données à caractère personnel est mis en œuvre ;

- attire l'attention s'agissant des transferts de données hors UE, en rappelant :
  - que l'hébergement dans l'UE/EEE ou dans un pays tiers adéquat permet notamment d'assurer un niveau de protection adéquat,
  - que même en cas de localisation dans l'UE, les données doivent être immunisées contre toute demande d'autorité de pays tiers en dehors d'un accord international conformément aux articles 28 et 48 du RGPD ;

- étaye le critère de « données d'une sensibilité particulière » nécessitant le respect de qualification SecNumCloud avec la notion de violation susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et à la vie des personnes, créant ainsi une définition à deux conditions : **(i) sensibilité par nature et (ii) sensibilité par risque et conséquence d'une violation de la donnée** ;

- restreint les données d'une sensibilité particulière aux :
  - **données relevant de secrets protégés par la loi**, notamment au titre des articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration (CRPA[10]) ;
  - **données nécessaires à l'accomplissement des missions essentielles de l'État**.

  Il convient de noter que la CNIL avait poussé à ce que la définition des données d'une sensibilité particulière inclue également une référence aux catégories particulières de données (article 9 du RGPD) et aux données relatives aux condamnations pénales et aux infractions (article 10 du RGPD). Cependant, la version publiée n'a pas retenu cette proposition ;

- maintient une dérogation transitoire pour les projets **déjà engagés** d'au maximum 12 mois, après validation du Premier ministre, à compter de la disponibilité d'une offre « acceptable ».

[10] C'est-à-dire notamment le secret des délibérations du Gouvernement, le secret de la défense nationale, le secret de l'instruction, le secret médical, le secret des affaires, etc.

[redacted]

177
178

[redacted]

204
205
206

[redacted]

[redacted]

4. Annexe A : Règle R9

R9 dans la Circulaire du 5 juillet 2021	**R9 dans la Circulaire du 31 mai 2023** (les parties soulignées sont les modifications par rapport à l'ancienne version)
Dans le cas d'un recours à une offre de *cloud* commerciale, les systèmes informatiques en production et en recette, incluant les éléments nécessaires à leur résilience, doivent respecter la règle suivante :	Dans le cas d'un recours à une offre de *cloud* commerciale, les systèmes informatiques en production et en recette, incluant les éléments nécessaires à leur résilience, doivent respecter la règle suivante :
- Tous les systèmes et applications informatiques manipulant des données à caractère personnel doivent **être conformes au RGPD**. Pour les systèmes contenant des données de santé, l'hébergeur doit de plus être **conforme à la législation sur l'hébergement de données de santé**.	Tous les systèmes et applications informatiques traitant des données à caractère personnel, y compris celles des agents publics, doivent être conformes au RGPD. <u>À ce titre, une attention particulière doit être portée à d'éventuels transferts de données à caractère personnel en dehors de l'UE et il est rappelé que l'hébergement sur le territoire de l'UE, de l'EEE, ou d'un pays tiers faisant l'objet d'une décision d'adéquation de la Commission européenne, adoptée en application de l'article 45 du RGPD, permet notamment d'assurer un niveau de protection adéquat aux données. Par ailleurs, même lorsque les données sont localisées dans l'Union, conformément aux articles 28 et 48 du RGPD, ces données doivent être immunisées contre toute demande d'autorité publique d'États tiers (judiciaire ou administrative) en dehors d'un accord international en vigueur entre le pays tiers demandeur et l'Union ou un État membre.</u> Pour les systèmes contenant des données de santé, l'hébergeur doit de plus être conforme à la législation sur l'hébergement de données de santé.
- Si le système ou l'application informatique manipule des données d'une sensibilité particulière, qu'elles relèvent notamment des données personnelles des citoyens français, des données économiques relatives aux entreprises	Si le système ou l'application informatique traite des données, à caractère personnel ou non, d'une sensibilité particulière et dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et la vie des personnes

françaises, ou d'applications métiers relatives aux agents publics de l'État : l'offre de *cloud* commercial retenue devra impérativement respecter la **qualification SecNumCloud** (ou une qualification européenne d'un niveau au moins équivalent) et **être immunisée contre toute réglementation extracommunautaire**. - Sinon, l'administration en charge du système choisit la solution adaptée en fonction de ses propres critères, en privilégiant chaque fois que possible une offre qualifiée SecNumCloud et immunisée aux réglementations extracommunautaires.	ou à la protection de la propriété intellectuelle, l'offre de *cloud* commerciale retenue devra impérativement respecter la **qualification SecNumCloud** (ou une qualification européenne garantissant un niveau au moins équivalent, notamment de cybersécurité) et être immunisée contre tout accès non autorisé par des autorités publiques d'État tiers. Dans le cas contraire, le recours à une offre de *cloud* commerciale qualifiée SecNumCloud et immunisée contre tout accès non autorisé par des autorités publiques d'État tiers n'est pas requis. Ces données d'une sensibilité particulière recouvrent : - **les données qui relèvent de secrets protégés par la loi**, notamment au titre des articles L. 311-5 et L. 311-6 du code des relations entre le public et l'administration (par exemple, les secrets liés aux délibérations du Gouvernement et des autorités relevant du pouvoir exécutif, à la défense nationale, à conduite de la politique extérieure de la France, à la sûreté de l'État, aux procédures engagées devant les juridictions ou encore le secret de la vie privée, le secret médical, le secret des affaires qui comprend le secret des procédés, des informations économiques et financières et des stratégies commerciales ou industrielles) ; - **les données nécessaires à l'accomplissement des missions essentielles de l'État**, notamment la sauvegarde de la sécurité nationale, le maintien de l'ordre public et la protection de la santé et de la vie des personnes. La violation des données décrites ci-dessus, susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique,

	à la santé et à la vie des personnes, ou à la protection de la propriété intellectuelle, devra être évaluée sous chaque angle des critères de sécurité élémentaires, à savoir : la confidentialité, l'intégrité, la disponibilité voire la traçabilité. Il pourra être pris en compte dans cette analyse différentes natures d'impacts possibles (par exemple notamment : impacts opérationnels, politiques, économiques, juridiques, environnementaux, patrimoniaux).
- A titre transitoire, pour les projets déjà engagés, une dérogation à ces deux derniers alinéas pourra être accordée sous la responsabilité du ministre dont relève le projet, sans qu'elle ne puisse aller au-delà de 12 mois après la date à laquelle une offre de *cloud* acceptable (c'est-à-dire dont les éventuels inconvénients sont supportables ou compensables) sera disponible en France.	À titre transitoire, pour les projets déjà engagés, une dérogation à l'alinéa précédent pourra être accordée sous la responsabilité du ministre dont relève le projet, et après validation du Premier ministre, sans qu'elle ne puisse aller au-delà de 12 mois après la date à laquelle une offre de *cloud* acceptable (c'est-à-dire dont les éventuels inconvénients sont supportables ou compensables) sera disponible en France.

Il est important de noter que le projet de référentiel de certification des services cloud en cours d'élaboration par l'ENISA prévoit un niveau de garantie dédié au traitement de « données d'une sensibilité particulière » dont la définition reprend exactement les mêmes termes que la règle R9.

5. Annexe B : Exemples d'organismes visés par la doctrine « *cloud* au centre »

Les circulaires du 5 juillet 2021 et du 31 mai 2023 prévoient que « *cette doctrine s'applique* ***aux acteurs de l'État et aux organismes placés sous sa tutelle****, comme retenus dans le décret 2019-1088 définissant le système d'information de l'État* » et sont introduites par un courrier du/de la Premier(-ère) ministre adressé aux ministres, ministres délégués et secrétaires d'État.

Le décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique définit celui-ci comme étant composé de l'ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker sous forme numérique les données qui concourent aux missions des services de l'État et des organismes placés sous sa tutelle.

Sont exclus du champ d'application de ce décret :

- les systèmes d'information opérationnels et de communication du SI de la défense[11] ;
- les systèmes d'information scientifiques et techniques du SI de la défense[12] ;
- les services opérés par la DGSE[13] ;
- les services opérés par la DGSI[14].

[redacted]

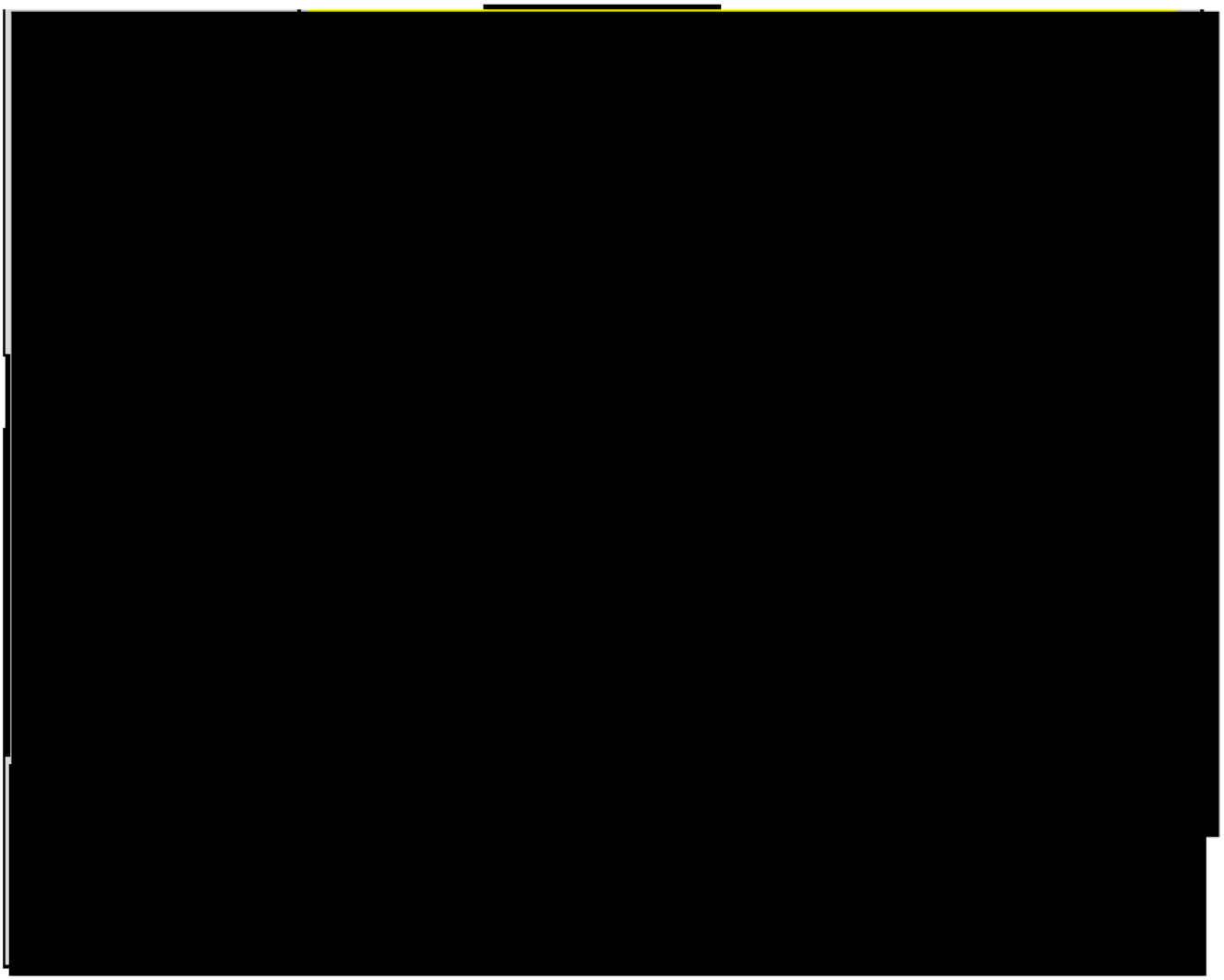
[redacted] Article 2 du décret n° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication

[12] Ibid

[13] Article D. 3126-2 du code de la défense

[14] Article 1er du décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure

[redacted]



6. Annexe C : Détails de la stratégie nationale pour le *cloud* (axes 1 & 3)

Axe 1 : Le « *cloud* de confiance » au travers de la qualification SecNumCloud de l'ANSSI

La qualification SecNumCloud garantit un niveau de sécurité élevé pour les prestataires de cloud.

La version 3.2 du 8 mars 2022 du référentiel SecNumCloud explicite des **critères de protection vis-à-vis de la législation extra-européenne** :

- le « siège statutaire, administration centrale et principal établissement » du prestataire dans l'UE ;
- des exigences sur le capital social du prestataire (le capital minimum que devraient détenir des acteurs européens est de 61 %) ;
- l'absence de possibilité technique par toute société hors UE intervenant dans le traitement d'accéder aux données traitées (y compris les données techniques).

La CNIL considère que SecNumCloud fournit **une réponse conforme *by design* aux exigences de la CJUE en matière de protection des données identifiés dans son arrêt Schrems 2** et elle recommande le recours à un prestataire de niveau SecNumCloud pour les responsables de traitement qui veulent garantir un haut niveau de protection des données à caractère personnel[15].

Par ailleurs, le Gouvernement a lancé fin 2022 un dispositif d'accompagnement à la qualification SecNumCloud pour les PME et start-ups de la sphère SaaS/PaaS[16], piloté par la DGE et la DGRI opéré par Bpifrance.

À ce jour, cinq fournisseurs sont qualifiés SecNumCloud :

- Cloud Temple : offre « Secure Temple » (IaaS) ;
- Oodrive : suite collaborative « Meet », « Work », et « Share » (SaaS) ;
- Outscale : offre « IaaS Cloud on Demand » (IaaS) ;
- OVH : offre « Private Cloud » (IaaS) ;
- Worldline : offre « Secured IaaS » (IaaS).

Selon le gouvernement, la stratégie nationale pour le *cloud* a permis aux administrations de doubler leur volume de marchés passés avec des offres SecNumCloud[17].

Six autres fournisseurs sont en cours de qualification :

- Cloud Solutions : suite collaborative « Wimi Entreprise » (SaaS) ;
- Idnomic : Infrastructure de clés publiques et identité numérique (SaaS) ;
- Index Education : Suite logicielle incluant Pronote (SaaS) ;

[15] L'ANSSI actualise le référentiel SecNumCloud : https://www.ssi.gouv.fr/actualite/lanssi-actualise-le-referentiel-secnumcloud/
[16] France 2030 : vers un renforcement de l'offre cloud de confiance https://presse.economie.gouv.fr/06042023-cp-france-2030-vers-un-renforcement-de-loffre-cloud-de-confiance/
[17] Un premier bilan positif : https://www.economie.gouv.fr/cloud-cinq-nouveaux-dispositifs-soutenir-developpement-secteur

- Cegedim : offre « CegNumCloud « (IaaS) ;
- Whaller : suite collaborative « Donjon » (SaaS) ;
- Orange : Cloud Avenue (IaaS).

Axe 3 : La stratégie d'accélération cloud

Dans le cadre du programme « France 2030 » et du programme d'investissements d'avenir 2021-2025, l'État soutient financièrement les projets industriels de développement de services *cloud* français (1,8 Md€).

Ce soutien s'est renforcé depuis septembre 2022, avec la définition de cinq nouvelles mesures[18] annoncées par le gouvernement pour poursuivre la stratégie d'accélération :

- l'accompagnement de l'ANSSI pour obtenir le label SecNumCloud pour les PME et start-ups proposant des services SaaS ou PaaS ;

- l'accompagnement des administrations – notamment celles traitant des données sensibles – dans leur migration vers le cloud via une mission d'appui pilotée par la DINUM ;

- la poursuite des travaux sur le schéma de certification de la sécurité du cloud (EUCS) porté par l'ENISA et sur le projet de règlement « Data Act » ;

- un soutien à l'innovation dans le *cloud* via un Projet Important d'Intérêt Européen Commun (PIIEC) dédié ;

- la création d'un Comité Stratégique de Filière numérique de confiance (CSF numérique), présidé par Michel Paulin, DG d'OVHcloud.

Un premier appel à projets concernant les « suites bureautiques collaboratives *cloud* », visant à soutenir le développement de suites collaboratives qualifiées SecNumCloud, a été ouvert au printemps 2022. Trois projets lauréats ont été annoncés en avril 2023 : Wimi, Jamespot et Interstis.

[18] Cloud : cinq nouveaux dispositifs pour soutenir le développement du secteur https://www.economie.gouv.fr/cloud-cinq-nouveaux-dispositifs-soutenir-developpement-secteur