La Première Ministre

Paris, le 31 MAI 2023

n° 6404/SG

à

Mesdames et Messieurs les ministres,
Mesdames et Messieurs les ministres délégués,
Mesdames et Monsieur les secrétaires d'État,

Objet : Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre »)

Lors du comité interministériel de la transformation publique du 9 mai dernier, j'ai pu rappeler toute l'importance de la mobilisation des leviers numériques pour un Etat plus simple et plus efficace.

La circulaire du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'Etat a fait entrer l'informatique de l'État dans une nouvelle ère en favorisant l'adoption de ce mode d'hébergement et de production informatique favorisant l'expérimentation et le passage à l'échelle ainsi que le travail collaboratif.

Dans le cadre de cette transformation, l'Etat veille scrupuleusement à la protection de ses données et de celles de nos concitoyens. La doctrine d'utilisation de l'informatique en nuage par l'Etat, introduite par la circulaire du 5 juillet 2021, exige ainsi, en cas de recours à une offre commerciale d'informatique en nuage, l'hébergement des données d'une sensibilité particulière par des solutions disposant de la qualification SecNumCloud délivrée par l'Agence nationale de sécurité des systèmes d'information (ou une qualification européenne d'un niveau au moins équivalent) et immunisées contre toute règlementation extracommunautaire.

Après plusieurs mois d'application de cette doctrine, il apparaît nécessaire d'en préciser les conditions d'application 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 requise ainsi que de préciser les modalités de demandes de dérogation à cette règle.

Je vous remercie d'apporter une attention particulière à la version actualisée de cette doctrine et je vous rappelle que la direction interministérielle du numérique se tient à disposition pour tout appui dans la mise en œuvre de cette doctrine.

Elisabeth BORNE

Doctrine « cloud au centre »
sur l'usage de l'informatique en nuage au sein de l'État

Version du 25 mai 2023

1. Historique

Le système d'information de l'État est régi par le décret n°2019-1088 du 25 octobre 2019. Il consacre à la fois une large délégation aux ministères de la responsabilité du Premier ministre dans la mise en œuvre des systèmes d'information relatifs aux politiques publiques qu'ils portent, et le rôle d'animation stratégique, de conseil, de coordination interministérielle et de mutualisation opéré par la direction interministérielle du numérique de l'État (DINUM), sous l'autorité du ministre de la transformation et de la fonction publiques. Ce rôle se traduit notamment par l'identification des bonnes pratiques et des innovations du marché numérique et l'impulsion à s'en saisir, dans le respect des intérêts des citoyens et de l'État.

Les opportunités relatives à l'informatique en nuage (*cloud*) ont donné lieu à une stratégie d'amorçage, formalisée dans une circulaire du 8 novembre 2018. Elle identifie le *cloud* comme l'un des chantiers prioritaires de la transformation numérique de l'État. Elle encourage les acteurs publics à s'emparer du *cloud* et à s'appuyer sur son potentiel pour rendre un meilleur service public aux citoyens, tout en gardant la maîtrise des données sensibles.

Les enjeux sous-jacents sont les suivants :

- - Enjeu de **transformation** pour l'État en ce que le *cloud*, en est le facilitateur structurel. L'adoption du *cloud* doit s'accompagner de celle des pratiques associées à l'excellence dans la production de services numériques (proximité entre métiers et équipes informatiques, scalabilité, agilité, « *devops* », « *continuous delivery* » qui sont les garants de l'adaptation des produits à leurs utilisateurs) ;
- - Enjeux de **souveraineté et de sécurité** : l'adoption du *cloud* ne doit pas entraver l'autonomie de prise de décision ni d'action de l'État, pas plus que sa sécurité numérique et la résilience de ses infrastructures, la maîtrise par l'État des données et des traitements qui lui sont confiés, le respect des règles européennes en matière de protection des données à caractère personnel, et ce alors que l'empreinte des acteurs extra-européens en matière de *cloud* est prédominante ;
- - Enjeu **industriel** : l'adoption du *cloud* par l'État, et plus généralement la sphère publique, doit être une opportunité pour l'écosystème français et européen avec comme bénéfice réciproque pour les acteurs publics d'accéder à une offre compétitive au niveau européen sinon mondial.

Le terme générique de *cloud* recouvre habituellement trois niveaux de services différents : l'hébergement distant « *Infrastructure as a Service* » (IaaS), l'appui sur des composants techniques mutualisés pour simplifier la fabrication d'applications « *Platform as a Service* » (PaaS), et l'accès en mode locatif à des logiciels « *Software as a Service* » (SaaS).

Nous distinguerons dans la suite deux finalités :

- - Le « *cloud* pour les équipes informatiques », qui recouvre les niveaux IaaS et PaaS ;
- - Le « *cloud* pour les utilisateurs », qui recouvre les services logiciels accédés par les agents publics en SaaS.

2. Situation début 2021

Les deux années écoulées ont permis de concrétiser la stratégie de la circulaire de 2018 et d'obtenir des résultats tangibles.

2.1. Concernant le « *cloud* pour les équipes informatiques »

L'État a en premier lieu mis en place une stratégie d'offre, visant à investir pour mettre à disposition des équipes informatiques les capacités techniques et contractuelles de souscription aux technologies d'infrastructures *cloud*.

1) Cloud interne de l'État

L'État, comme la plupart des grandes organisations privées, s'est doté d'un ***cloud* interne** (dit « cercle 1 » dans la circulaire de 2018). Ces infrastructures, entièrement maîtrisées par l'État, incluant hébergement, ingénierie, exploitation et surveillance, visent à héberger les traitements et les données sensibles, ou dont la compromission nuirait au bon fonctionnement de l'État.

Il prend la forme de deux offres de services conçues, hébergées, exploitées et surveillées par :

- le ministère de l'Intérieur (*cloud* PI), associé à un niveau de sécurité « Diffusion restreinte »
- le ministère des finances (*cloud* NUBO), associé au standard SecNumCloud (qualification ANSSI de référence)

Ces offres, qui s'appuient sur la technologie *open source* OpenStack, atteignent des résultats à saluer : une taille critique suffisante pour permettre leur viabilité, une ouverture aux besoins interministériels, des coûts et performances qui, sans atteindre encore le niveau des acteurs industriels spécialistes, rendent l'usage acceptable pour des besoins dont le niveau de sécurité le justifie.

Elles s'appuient sur, et sont portées par, le réseau interministériel de l'État (RIE), dont la raison d'être est d'assurer la continuité de l'État, même en cas de défaillance majeure d'Internet, et dont la résilience va être encore renforcée dans les années à venir.

Elles ont vocation à couvrir les besoins de «*cloud* interne» de l'ensemble des ministères et à héberger une instance de tout système d'information indispensable pour la continuité de l'État, à l'exclusion de ceux du ministère des Armées qui dispose de son propre *cloud* interne adapté aux exigences de ses systèmes d'information opérationnels, et de ceux qui ne sont pas déployés sur le RIE.

Elles doivent continuer à évoluer (résilience, richesse des briques PaaS, qualité de la relation client, etc.), avec notamment le projet d'introduction d'une offre d'orchestration de *containers*.

Elles doivent continuer à s'appuyer sur des technologies standard qui garantissent leur réversibilité vers les autres offres de *cloud* internes ou commerciales. Elles doivent également continuer à s'appuyer sur un modèle économique, donnant lieu à un coût de refacturation aux administrations utilisatrices cohérent avec le coût réel de ces offres.

Cet état des lieux valide la stratégie initiale engagée en matière de *cloud* interne et l'opportunité de la poursuite de leur développement, en veillant à ce que les efforts des ministères dans la construction et le développement de *cloud* interne (hors maintenance de l'existant) soient exclusivement dirigés sur ces deux offres.

2) *Cloud* commercial

L'État a mis en place, via la centrale d'achat public UGAP, un support contractuel d'achat regroupant des offres commerciales « sur étagère » de fournisseurs de *cloud* spécialisés, en conformité avec le niveau dit « cercle 3 » dans la circulaire de 2018. Il vise à offrir le meilleur de l'état de l'art, sans prérequis de sécurité et de souveraineté (entendu dans le sens d'une indépendance au droit extra-européen), ce qui n'empêche pas que certaines offres commerciales aient d'excellentes qualités en la matière et puissent encore s'améliorer avec le temps.

Ces offres présentent d'ores et déjà un continuum de fonctionnalités et, pour partie, un niveau de conformité en matière de sécurité (SecNumCloud) qui permet de couvrir une large gamme de besoins de l'État. Elles ont vocation à continuer à progresser sur les plans fonctionnels, sécuritaires, d'interconnexion avec le RIE, à l'initiative des industriels concernés ou en partenariat avec les administrations.

3) Appui à la consommation des offres *cloud*

Dans le même temps, la DINUM a engagé auprès de l'ensemble des administrations une stratégie de soutien à la consommation des offres *cloud* précitées, *via* des leviers d'expertise, de co-financement et d'appui à la gouvernance.

Elle s'est également traduite par la simplification du parcours de commande pour les équipes informatiques des administrations, afin de favoriser la découverte et le recours à l'offre commerciale.

En quelques mois, plus de 200 projets ont déclaré leur intérêt pour les offres de *cloud* commercial et engagé leur bascule. Plusieurs projets d'envergure ont été déployés ou sont en cours de déploiement sur le *cloud* interne de l'État.

2.2. Concernant le « *cloud* pour les utilisateurs »

La bascule de services de l'État vers des logiciels à la demande dans le *cloud* s'effectue spontanément. Plateformes collaboratives, messagerie, portails de dématérialisation de démarches, logiciels métiers : les éditeurs de logiciels utilisés par l'État ont tous ouvert une offre SaaS et incitent les administrations à y souscrire.

Ce phénomène, qui se constate également dans la plupart des entreprises, est l'occasion pour les services utilisateurs de s'approprier des solutions qui répondent à leurs attentes fonctionnelles.

Ce mouvement doit être accompagné pour faciliter l'identification des offres logicielles à la demande qui répondront le mieux aux enjeux simultanés d'ergonomie, de richesse fonctionnelle, de sécurité, de protection des données, de facilité d'utilisation, de souveraineté et de maitrise de la dépense publique. Cet accompagnement doit également être l'occasion d'identifier les opportunités de mutualisation pour réaliser des économies d'échelle ou des gains opérationnels.

Les directions du numérique de l'État l'ont bien compris et ont engagé cette évolution. Dans le même temps, la DINUM a engagé la constitution d'une offre de services numériques interministériels, accessibles à tous les agents publics, construite sur des plateformes *cloud* IaaS et PaaS internes et commerciales. Cette suite collaborative interministérielle comporte déjà plusieurs services collaboratifs (messagerie instantanée Tchap, messagerie collaborative de l'État, services collaboratifs Resana et Osmose, plateforme d'audioconférence Audioconf, webconférence) et s'étoffera.

3. Mise à jour de la doctrine *cloud* de l'État

Ces progrès et l'évolution des offres du marché, désormais nombreuses, de grande qualité et conciliant les enjeux de performance et de plus grande souveraineté, permettent de faire évoluer la doctrine *cloud* de l'État vers une approche nommée « *cloud* au centre ».

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 se focalise sur deux grands enjeux :

- Développer la demande de *cloud* au sein des équipes informatiques et des services utilisateurs, en bénéficiant des offres désormais disponibles ;
- Focaliser l'attention et les efforts sur l'accompagnement des métiers et des équipes de développement de produits numériques au sein de l'État, afin d'adapter les processus et les compétences des acteurs au potentiel du *cloud* et aux points d'attention propres à ces offres. Ce faisant, il s'agit d'internaliser au sein de l'État la compréhension et la compétence, afin d'orienter le flux de nouveaux projets vers le *cloud*, plutôt que de focaliser l'attention sur le stock en continuant à construire de nouveaux projets avec les méthodes du XX^{e} siècle.

3.1. Concernant le développement de la « culture cloud »

[R1] Pour tout nouveau projet numérique, quelle que soit sa taille, une solution *cloud* doit être recherchée : si le « *cloud* pour les utilisateurs » ne permet pas de remplir le besoin, une solution dédiée doit être envisagée sur une plateforme du « *cloud* pour les équipes informatiques ». Dans les deux cas, le mode produit doit être privilégié, incluant l'autonomie des équipes, la prise en charge continue des opérations, la confrontation rapide avec les utilisateurs du produit et un jalonnement par l'impact permettant d'arrêter, d'infléchir ou d'accélérer la trajectoire du produit en fonction des résultats constatés.

[R2] Les recrutements et les programmes de formation continue d'agents relevant à la fois des équipes informatiques et des directions sponsors des projets et des produits numériques, devront comporter un volet *cloud*. Il en va de même pour leurs managers. Les équipes qui expérimentent pour la première fois les approches *cloud* pourront bénéficier d'un accompagnement spécifique, mis en place par leur ministère, avec l'appui de la DINUM.

[R3] Il appartient à chaque administration de mettre en place les processus d'incitation et de contrôle de cette politique, qui mesure le niveau d'adoption par les équipes, identifie les freins et tient à jour le plan d'action visant à leur levée.

[R4] Tout projet relevant d'offres *cloud* commerciales devra comporter des conditions de fin de contrat et de réversibilité soutenables pour son administration, et provisionner les ressources financières, techniques et humaines correspondantes dès le lancement du projet, afin de rendre cette réversibilité activable effectivement.

L'adéquation avec les règles[1] de GAIA-X, notamment d'interopérabilité et de portabilité, devra également être recherchée dans la mesure du possible.

[R5] Tout projet numérique ayant recours au *cloud* doit respecter les meilleures pratiques en matière de résilience, et reposer a minima sur des services déployés dans plusieurs zones géographiques pour assurer, selon le niveau de criticité, la continuité ou la reprise d'activité dans les meilleures conditions. L'offre *cloud* mobilisée doit offrir des garanties satisfaisantes en matière de mise à jour de ses composants pouvant être affectés par des failles de sécurité ainsi que de transparence et de réactivité en cas de compromission. En outre, lorsqu'elle envisage de retenir une offre *cloud* commerciale, l'administration doit prendre les mesures nécessaires de détection et d'isolation liées à la prévention de la propagation d'une compromission de sécurité.

3.2. Concernant le « *cloud* pour les équipes informatiques »

[R6] Pour tout nouveau projet informatique, les équipes informatiques de l'État et leurs prestataires doivent par défaut s'appuyer sur une ou plusieurs des offres de *cloud* internes ou commerciales pour couvrir l'intégralité du cycle de production des applications (développement, recette, production, secours, éventuelles plateformes bac à sable et formation). Les ministères choisissent, en fonction de critères qui leur sont propres, et notamment le niveau de sécurité, le coût complet de possession, l'expertise RH dont ils disposent en leur sein, leurs besoins techniques et fonctionnels, les choix d'urbanisation préalables, s'ils recourent pour leurs produits numériques au *cloud* interne de l'État ou à une offre *cloud* commerciale. Cette règle s'applique par extension à tout produit numérique existant qui donne lieu à une évolution majeure (changement de prestataire, évolutions représentant au moins 50 % du coût de fabrication du produit initial).

[R7] Les équipes qui souhaitent déroger à [R6] doivent le documenter auprès de la DINUM pour tout projet présentant un coût complet d'au moins un million d'euros, en produisant une étude comparative sur les aspects économiques, juridiques, métiers et de sécurité entre les scénarios.

[R8] Le contrôle de la doctrine « *cloud* au centre » est désormais intégré à la procédure de contrôle de conception des grands projets informatiques de l'État issue de l'article 3 du décret n°2019-1088 du 25 octobre 2019, au-delà du seuil de neuf millions d'euros. Sous ce seuil, ce contrôle relève des ministères.

[R9] 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 :

---

[1] GAIA-X: Policy Rules and Architecture of Standards (data-infrastructure.eu)

Tous les systèmes et applications informatiques traitant des données à caractère personnel, y compris celles des agents publics, doivent être conformes au RGPD. A 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'Etats tiers (judiciaire ou administrative) en dehors d'un accord international en vigueur entre le pays tiers demandeur et l'Union ou un État membre. 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 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 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'Etat 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'Etat, 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).

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.

[R10] La portabilité multi-*clouds* doit être assurée. A cette fin, les équipes informatiques s'assureront que les adhérences techniques et fonctionnelles à la plateforme *cloud* retenue n'entravent pas notablement cette capacité de réversibilité et de changement de fournisseur de *cloud*. Dans le cas où cette adhérence est néanmoins légitimée par des gains opérationnels immédiats, le surcoût de la réversibilité doit être financé par ces gains.

3.3. Concernant le « *cloud* pour les utilisateurs »

[R11] La DINUM est chargée de piloter, avec le concours des DNUM, la conception et la mise en œuvre de l'offre en matière d'outils collaboratifs interministériels, accessible à la demande par tous les agents de l'État.

[R12] Les ministères peuvent proposer à leurs agents des services logiciels à la demande additionnels à ceux disponibles dans la suite collaborative interministérielle. Ces offres doivent répondre aux attentes de leurs utilisateurs, tout en s'inscrivant dans les moyens humains et financiers dont les ministères disposent. Les ministères sont incités à se regrouper et à mutualiser leurs moyens à cet effet, avec l'appui de la DINUM, sans que cela ne conduise à empêcher les agents d'accéder à la suite collaborative interministérielle.

[R13] Les administrations ne doivent pas chercher à créer et maintenir de nouveaux logiciels sur mesure qui trouvent déjà leur équivalent dans les sphères publique ou privée ou parmi les communs numériques contributifs (logiciels libres et plateformes de services collaboratifs libres et ouverts, par exemple). Elles doivent répondre aux besoins de leurs agents et des citoyens en privilégiant les solutions disponibles, soit en y recourant sous forme de souscription de logiciel à la demande (offres SaaS commerciales), soit en intégrant, adaptant et déployant ces solutions sur le *cloud* interne de l'État (offres SaaS internes). En l'absence de solutions sur étagère, elles peuvent engager un développement sur mesure limité au périmètre spécifique en question.

[R14] Pour les services précités en [R11] et [R12], la conformité des infrastructures et des services de l'éditeur à la règle [R9] est impérative.

[R15] Dans le respect des règles de la commande publique, la diversité des fournisseurs doit être recherchée à l'échelle de l'État sur chaque segment des services aux utilisateurs, pour éviter la création de marchés captifs. Les administrations doivent, chaque fois que possible, évaluer plusieurs offres couvrant leurs besoins, en particulier dans les domaines de la micro-informatique, de la bureautique, de la messagerie et des solutions collaboratives.