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.

"*Cloud first*" doctrine :
The use of cloud computing within the public sector

Version of May 25, 2023

1.Historical Context

The government information system is ruled by Decree no. 2019-1088 of October 25, 2019. It establishes a major delegation of the Prime Minister's responsibility for the implementation of public policy information systems to the ministries. The role of strategic leadership, advice, interministerial coordination and pooling is performed by the interministerial Digital Direction, under the authority of the minister of public transformation and public function. This role involves identifying best practices and innovations in the digital marketplace, and encouraging their use, while respecting the interests of citizens and the State

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.

The opportunities associated with cloud computing have given rise to an initiation strategy, formalized in a circular dated 8 November 2018. It identifies the cloud as one of the priority projects for the digital transformation of the State. It encourages public actors to adopt the cloud and exploit its potential to provide better public services to citizens, while maintaining control over sensitive data.

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, aginté, « *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.

The underlying issues are:

- The cloud is the structural enabler of the State's **transformation**. The adoption of the cloud must be accompanied by the adoption of practices associated with excellence in the production of digital services (proximity between business and IT teams, scalability, agility, devops and continuous delivery, which guarantee that products are adapted to their users) ;
- **Sovereignty and security** issues: at a time when the presence of non-European cloud players is predominant, the adoption of the cloud must not interfere with that of the state:
    - autonomy of decision making or action ;
    - digital security and infrastructure resilience ;
    - control over the data and processing entrusted to It ;
    - compliance with European legislation on personal data protection.
- **Industrial considerations**: the adoption of the cloud by the State, and more generally by the public sector, should be an opportunity for the French and European ecosystem, with the public sector players benefiting from access to a competitive offer at European and global level.

Le terme générique de *cloud* recouvre habituellement trois niveaux de services différents : l'hébergement distant « *Infrastructure as a Service* » (laaS), 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 « *So~ware as a Service* » (SaaS).

Nous distinguerons dans la suite deux finalités :

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

The generic term "cloud" usually covers three different levels of service:

- "Infrastructure as a Service" (laaS) remote hosting;
- "Platform as a Service" (PaaS) shared technical components to simplify application production;
- "Software as a Service" (SaaS) rental software access.

In the following text, we will distinguish between two purposes:

- “Cloud for IT teams", covering the laaS and PaaS levels;
- “Cloud for users", covering SaaS software services accessed by public sector employees.

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.

2. Situation at the beginning of 2021

Over the past two years, the 2018 circular strategy has been put into practice and tangible results have been achieved.

2.1. Cloud for IT teams

First and foremost, the French government has put in place a supply strategy that aims to invest in providing IT teams with the technical and contractual capacity to subscribe to cloud infrastructure technologies.

1) Private interministerial cloud

Like most large private organisations, the French State has set up a **private cloud** (referred to as "Circle 1" in the 2018 Circular). These infrastructures, which are fully under the control of the State, including hosting, engineering, operation and monitoring, are designed to host sensitive data and processing, or data whose compromise would be detrimental to the proper functioning of the State. It takes the form of two service offerings designed, hosted, operated and monitored by :

- The Ministry of the Interior (cloud PI), associated with a “Restricted diffusion” security level ;
- The Ministry of Finance (cloud NUBO), associated with the *SecNumCloud*[1] standard (*ANSSI*[2] reference qualification).

These offerings, based on OpenStack open-source technology, are achieving good results : sufficient critical mass to ensure their viability, openness to interdepartmental needs, and costs and performance that, while not yet reaching at the level of industrial players, make them acceptable for use where the level of security justifies it.

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.

---

[1] SecNumCloud is a safety visa developped by the ANSSI which is the National Cybersecurity Agency of France. More information about SecNumCloud: https://www.ssi.gouv.fr/actualite/zoom-sur-secnumcloud-et-la-protection-des-donnees/

[2] ANSSI: The National Cybersecurity Agency of France

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.

They are based on, and supported by, the interministerial network based on internal infrastructure, whose mission is to ensure the continuity of the State, even in the event of a major Internet failure, and whose resilience will be further strengthened in the coming years.

They are intended to cover the private cloud needs of all the ministries and to host an instance of any information system essential to the continuity of the State, with the exception of those of the Ministry of the Armed Forces, which has its own internal cloud adapted to the needs of its operational information systems, and those that are not deployed on the interministerial network based on internal infrastructure. They need to evolve (resilience, richness of PaaS building blocks, quality of customer relationships, etc.), in particular with the planned launch of a container orchestration offering.

They must continue to be based on standard technologies that guarantee their reversibility to other internal or commercial cloud offerings. They must also continue to be based on a business model that allows user management to be charged at a cost that reflects the true cost of these offerings.

This assessment confirms the initial private cloud strategy and the desirability of developing it further, while ensuring that ministries' efforts to build and develop a private cloud (excluding the maintenance of existing systems) are focused exclusively on these two offerings.

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 âvec 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.

2) Commercial cloud

The French State, through the UGAP public purchasing center, has set up a contractual purchasing support system that brings together "off-the-shelf" commercial offers from specialised cloud providers, in line with the level referred to as "Circle 3" in the 2018 Circular. It aims to offer the best of the state of the art, with no security or sovereignty requirements (in the sense of independence from non-European law), which does not prevent certain commercial offers from having excellent qualities in this area and from improving over time. These offerings already offer a range of functionalities and, in some cases, a level of security compliance (SecNumCloud) that covers a wide range of government needs. They will continue to evolve in terms of functionality, security and interconnection with the interministerial network based on internal infrastructure, on the initiative of the manufacturers concerned or in partnership with administration.

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.

3) Consumer support

At the same time, the Interministerial Digital Direction has embarked on a strategy to support all government agencies in their use of the above-mentioned cloud offerings, through expertise, co-financing and government support.

It has also simplified the ordering process for government IT teams, to encourage discovery and use of the commercial offering. In just a few months, more than 200 projects have expressed an interest in commercial cloud offerings and have started the migration process. Several major projects have been or are in the process of being deployed on the private clouds.

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 ci.ans 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 interministériel$, accessibles à tous les agents publics, construite sur des plateformes cloud laaS 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.

2.2 Cloud for users

State services are spontaneously moving to on-demand software in the cloud. Collaboration platforms, messaging, dematerialization portals, business software: the software publishers used by the State have all launched a SaaS offer and are encouraging administrations to subscribe. This phenomenon, which can also be observed in most companies, is an opportunity for user departments to find solutions that meet their functional expectations.

This trend needs to be supported to help identify the on-demand software offerings that best meet the simultaneous challenges of ergonomics, functionality, security, privacy, usability, sovereignty and control of public expenditure. This support should also provide an opportunity to identify opportunities for pooling resources to achieve economies of scale or operational benefits.

The State's digital departments have understood this and have embarked on this evolution. At the same time, the Interministerial Digital Direction has launched the creation of a set of interministerial digital services accessible to all civil servants, based on internal and commercial cloud LaaS and PaaS platforms. This interministerial collaboration toolkit already includes several collaboration services (Tchap : instant messaging, State collaborative messaging, Resana and Osmose : collaboration services, Audioconf : audio conferencing platform and web conferencing) and will be further developed.

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 XXe siècle.

3. Updating the French government's cloud doctrine

These advances and the development of market offerings, which are now numerous and of high quality, and which reconcile the challenges of performance and greater sovereignty, mean that the government's cloud doctrine is evolving towards a "cloud first" approach.

This doctrine applies to state actors and organizations under their supervision, as maintained in Decree 2019-1088 defining the state information system, and focuses on two main challenges:

- Develop demand for cloud among IT teams and user departments by taking advantage of the offerings now available ;
- Focus attention and effort on supporting the state's businesses and digital product development teams to adapt processes and skills to the potential of the cloud and the specific attention points associated with these offerings. The aim is to internalize the understanding and skills within the state to guide the flow of new projects towards the cloud, rather than focusing on the stock by continuing to build new projects using 20th century methods.

3.1. Concernant le développement de la « culture cloud »

3.1 Cloud culture development

[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.

[R1] For any new digital project, regardless of size, a cloud solution should be sought : if the "cloud for users" does not meet the needs, a dedicated solution on a "cloud for IT teams" platform should be considered. In both cases, the product mode should be favoured, in particular regarding team autonomy, continuous operational support, rapid confrontation with product users and impact-based milestones that allow the product trajectory to be halted, redirected or accelerated according to the results observed.

[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.

[R2] Recruitment and training of both IT teams and the departments that support digital projects and products should include a cloud component. The same goes for their managers.

Teams experimenting with cloud approaches for the first time will be able to benefit from specific support set up by their department, with the support of the Interministerial Digital Direction.

[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.

[R3] It is up to each administration to put in place the processes to promote and monitor this policy, measuring the level of adoption by teams, identifying any barriers and keeping the action plan to address them up to date.

[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 de GAIA-X, notamment d'interopérabilité et de portabilité, devra également être recherchée dans la mesure du possible.

[R4] Any project involving commercial cloud services must include end-of-contract and reversibility conditions that are sustainable for its management, and must provide the appropriate financial, technical and human resources from the outset of the project to enable reversibility to be activated effectively.

Wherever possible, the GAIA-X rules should also be respected, particularly regarding interoperability and portability.

[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 où 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.

[R5] Any digital project using the cloud must comply with best practices in terms of resilience and, at the very least, be based on services deployed in several geographical zones to ensure continuity or resumption of activity under the best possible conditions, depending on the level of criticality. Cloud services must offer satisfactory guarantees in terms of updating components that could be affected by security breaches, as well as transparency and responsiveness in the event of a compromise. In addition, when considering the use of a commercial cloud offering, local authorities must take the necessary detection and isolation measures to prevent the propagation of a security compromise.

3.2. Concernant le « cloud pour les équipes informatiques »

3.2 Cloud for IT teams

[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 doud 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).

[R6] For all new IT projects, governmental IT teams and their service providers must, by default, rely on one or more in-house or commercial cloud offerings to cover the entire application production cycle (development, acceptance, production, backup, any sandbox platforms and training). Depending on their own criteria, including security levels, total cost of ownership, internal staff expertise, technical and functional requirements, and prior urbanisation decisions, ministries choose whether to use the internal cloud or a commercial cloud offering for their digital products. By extension, this rule applies to any existing digital product that undergoes a major upgrade (change of service provider, upgrades representing at least 50% of the manufacturing cost of the original product).

[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.

[R7] Teams wishing to break from [R6] must document this to the Interministerial Digital Direction for any project with a total cost of at least one million euros and provide a comparative study of the economic, legal, business and security aspects between the scenarios.

[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.

[R8] As a result of article 3 of decree no. 2019-1088 of 25 October 2019, the control of the "cloud first" doctrine is now integrated into the design control procedure for major governmental IT projects above nine million euros. Below this limit, this control is the responsibility of the ministries.

[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 :

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 Gudiciaire 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 9es 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 pouvoi~ 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.

[R9] When using a commercial cloud offering, production and acceptance IT systems, including the elements necessary for their resilience, must comply with the following rule:

All IT systems and applications that handle personal data, including that of public officials, must comply with the GDPR. In this context, particular attention must be paid to any transfer of personal data outside the EU, and it is recalled that hosting in the territory of the EU, the EEA or a third country that is the subject of an adequacy decision by the European Commission, adopted in accordance with Article 45 of the GDPR, in particular, makes it possible to ensure an adequate level of data protection. Moreover, even if the data are located in the Union, they must be immune from any request, in accordance with Articles 28 and 48 of the GDPR. For systems containing health data, the host must also comply with the legislation on the hosting of health data.

If the IT system or application processes data, whether personal or not, that is particularly sensitive and whose compromise is likely to result in a breach of public order, public security, the health and life of individuals or the protection of intellectual property, the selected commercial cloud offering must meet the SecNumCloud qualification (or a European qualification guaranteeing at least an equivalent level, in particular in terms of cybersecurity) and be immune to unauthorised access by third party public authorities. Otherwise, the use of a SecNumCloud-qualified commercial cloud offering that is immune from unauthorised third-party access is not required.

This particularly sensitive data includes:

- data relating to legally protected secrets, in particular in accordance with articles L.311-5 and L.311-6 of the French Code of relations between the citizen and the administration (e.g. secrets relating to the deliberations of the government and executive authorities, national defence, the conduct of French foreign policy, State security, judicial proceedings or the confidentiality of private life, medical secrecy, business secrecy, including the confidentiality of processes, economic and financial information and commercial or industrial strategies) ;
- data necessary for the performance of essential state functions, in particular the safeguarding of national security, the maintenance of public order and the protection of the health and life of individuals.

Any violation of the data described above, which may affect public order, public security, the health and life of individuals or the protection of intellectual property, must be assessed from all angles of

the basic security criteria, i.e. confidentiality, integrity, availability and traceability. This analysis may take into account different types of potential impact (e.g. operational, political, economic, legal, environmental, patrimonial).

As a transitional measure, for projects already underway, a derogation from the previous paragraph may be granted under the responsibility of the minister in charge of the project and after validation by the Prime Minister, but no later than 12 months after the date on which an acceptable cloud offering (i.e. one whose potential drawbacks are tolerable or compensable) becomes available in 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.

[R10] Multi-cloud portability must be ensured. To this end, IT teams will ensure that technical and functional adherence to the chosen cloud platform does not significantly impede this ability to revert and change cloud provider. In cases where this adherence is nevertheless motivated by immediate operational benefits, the additional costs of reversibility must be financed by these benefits.

3.3. Concernant le « cloud pour les utilisateurs »

3.3 Cloud for users

[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.

3.3 Cloud for users

[R11] The Interministerial Digital Directorate, in collaboration with its counterparts in the government departments, is responsible for designing and implementing interministerial collaboration tools that are accessible to all government employees on demand.

[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.

[R12] Ministries can offer their staff on-demand software services in addition to those available in the interdepartmental collaboration toolkit.

These services must meet the expectations of their users, while fitting within the human and financial resources available to ministries. Ministries are encouraged to join forces and pool their resources for this purpose, with the support of the Interministerial Digital Direction, without this having the effect of preventing agents from accessing the inter-ministerial collaboration toolkit.

[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.

[R13] Governments should not seek to create and maintain new bespoke software that already exists in the public or private sector or in the digital commons (e.g. free software and free and open collaborative service platforms). They must respond to the needs of their employees and citizens by prioritising available solutions, either in the form of on-demand software subscriptions (commercial SaaS offerings) or by integrating, adapting and deploying these solutions in the internal cloud. In the absence of off-the-shelf solutions, they can undertake bespoke development limited to the specific scope in 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.

[R14] For the services mentioned in [R11] and [R12], it is imperative that the editor's infrastructure and services comply with rule [R9].

[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.

[R15] In compliance with public procurement rules, a diversity of suppliers must be sought at government level for each segment of user services to avoid the creation of captive markets. Wherever possible, public authorities should evaluate multiple offers to meet their needs, particularly in the areas of microcomputing, office automation, messaging and collaborative solutions.