// MARS 2019

10 CLÉS

pour l'Acheteur Public de Cloud

GUIDE PRATIQUE

#NATIONCLOUD

CISPE.cloud en partenariat avec EuroCloud FRANCE

AVANT-PROPOS

L'utilisation d'un modèle de « Cloud computing » est un pilier majeur de la transformation numérique de l'État. Il permet notamment une mise à jour et une amélioration permanente des infrastructures et des services tant sur le plan de la sécurité, des fonctionnalités ou encore de la stabilité. Il permet également une adaptation au plus juste des ressources utilisées à la hausse comme à la baisse, et ce de manière extrêmement rapide.

Le modèle d'achat public est un élément clé de réussite de la stratégie cloud de l'État. Il conditionne le processus d'adoption et d'utilisation de l'informatique en nuage et doit, dans ce sens, en être un facilitateur. Cependant, l'acquisition de technologies en nuage diffère de la plupart des acquisitions de technologies traditionnelles connues du secteur public. Les approches en matière d'achat doivent donc être repensées.

Le gouvernement français a publié sa stratégie cloud et demande à chaque acteur public sa mise en application concrète. Par conséquent, les acteurs publics, tels que l'union des groupements d'achats publics (UGAP) - en coordination avec la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) et la direction des achats de l'État (DAE) -, cherchent activement à comprendre les pratiques d'acquisition de ce type de technologies, les standards et les écueils à éviter.

La bonne compréhension du modèle cloud et de ses intérêts multiples crée un intérêt supplémentaire sur la phase de contractualisation et les éléments contractuels, identifiant les rôles et les responsabilités de chacun qui doivent être clairement identifiées et acceptées.

Ce document décrit 10 clés concrètes de modèle d'achat à prendre en compte pour pouvoir bénéficier au mieux des avantages du cloud.

SOMMAIRE

URL de téléchargement du document :
Cispe.cloud/PublicProcurement/France & Eurocloud.fr/NationCloud

EuroCloud FRANCE

CISPE.cloud

1 COMPRENDRE LES DIFFÉRENTS MODÈLES DE CLOUD ET DÉFINIR LE PÉRIMÈTRE DE L'ACHAT

Différents modèles de technologies cloud existent comme en témoigne la circulaire publiée par le gouvernement le 8 novembre 2018 définissant la stratégie de l'État en 3 cercles. Chacun de ces cercles intègre ses propres critères de partage de responsabilité, de gestion opérationnelle, de tarification ou de gestion de la sécurité.

Pour comprendre les exigences pertinentes à inclure dans une consultation cloud, il faut comprendre qu'il existe des modèles de déploiement et d'utilisation différents tels que les modèles privé, communautaire, public et hybride ainsi que IaaS, PaaS et SaaS[1] :

- **Infrastructure en tant que service (IaaS)** : la fonctionnalité proposée à l'acteur public consiste à fournir des ressources de traitement, de stockage, de réseaux et autres ressources informatiques fondamentales permettant à l'acteur public de déployer et d'exécuter des logiciels de son choix, ce qui peut inclure des systèmes d'exploitation et des applications. L'acteur public ne gère ni ne contrôle l'infrastructure cloud sous-jacente, mais il contrôle les systèmes d'exploitation, le stockage, les applications déployées et, éventuellement, de manière limitée, certains composants réseau (pare-feu hôtes, par exemple).

- **Plate-forme en tant que service (PaaS)** : la fonctionnalité fournie à l'acteur public consiste à déployer sur l'infrastructure cloud des applications créées par l'acteur public ou acquises et créées à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur.

L'acteur public ne gère ni ne contrôle l'infrastructure cloud sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais il contrôle des applications déployées et, éventuellement, des paramètres de configuration de l'environnement d'hébergement d'application

- **Logiciel en tant que service (SaaS)** : la fonctionnalité fournie à l'acteur public consiste à utiliser les applications du fournisseur s'exécutant sur une infrastructure cloud. Les applications sont accessibles depuis plusieurs périphériques client via une interface client léger comme un navigateur Web (par exemple, une messagerie Web) ou une interface de programme. L'acteur public ne gère ni ne contrôle l'infrastructure cloud sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation, le stockage ou mêmes les fonctionnalités d'applications individuelles, à l'exception possible de paramètres limités de configuration d'application spécifiques à l'utilisateur.

Il convient donc pour le pouvoir adjudicateur de faire une étude croisée de ses besoins et des services existants sur le marché pour y répondre (certains services regroupant plusieurs de ces trois modèles), et de privilégier un modèle "multi-cloud" où une organisation utilise une combinaison de fournisseurs pour ces différents modèles.

[1] Le site web de l'institut NIST fournit informations et normes reconnues au plan international sur ces types de services cloud : http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

2 CLARIFIER LE RÔLE ET LES RESPONSABILITÉS DE CHAQUE PARTIE

L'ensemble des parties prenantes au marché doivent avoir une lecture claire de l'organisation mise en œuvre dans le modèle d'acquisition du cloud. De tous les aspects de l'achat de cloud que nous citons comme bonnes pratiques, la compréhension de la matrice de responsabilité est sans aucun doute l'élément le plus important.

Le modèle de matrice de responsabilité est la pierre angulaire sur laquelle sera défini l'ensemble des processus opérationnels : gestion de la sécurité, des configurations, des consommations, et autres.

Il est important de comprendre que le contexte cloud ne permet pas de reprendre les modèles traditionnels tel qu'ITIL[2].

***Exemple** : le fournisseur de technologies cloud (Cloud Service Provider en anglais ou CSP) offre des capacités de chiffrement, mais il est de la responsabilité du client ou d'un partenaire d'activer la fonctionnalité sur les données qui lui semble le nécessiter.*

Cet exemple, parmi d'autres, illustre comment le modèle cloud remet à plat les matrices de responsabilités traditionnelles.
Il est donc nécessaire de prévoir des ateliers autour de cette question lors de la phase de contractualisation afin de permettre à l'acheteur public de mieux appréhender le changement organisationnel.

La politique d'achat doit donc redéfinir les processus opérationnels adaptés au contexte du cloud et répartir les responsabilités de ces processus sur les différents intervenants opérationnels : CSP, partenaires, distributeurs et bénéficiaires.

[2] ITIL (Information Technology Infrastructure Library) pour «Référentiel pour l'infrastructure des technologies de l'information», est un ensemble d'ouvrages recensant les bonnes pratiques (best practices) pour la gestion des services informatiques (ITSM), édictées par l'Office public britannique du Commerce (OGC).

Les questions à se poser pour délimiter les responsabilités de chaque acteur seront : Qui achète ? Qui contractualise ? Qui exploite ? Qui budgète ? Qui met en place les contrôles de sécurité et de dépenses ? Qui « distribue » ? Quel est le modèle économique des acteurs (revendeur, intégrateur, centrale d'achat) ?

Le schéma ci-dessous explique les différents rôles (NB : une même organisation peut avoir plusieurs rôles).

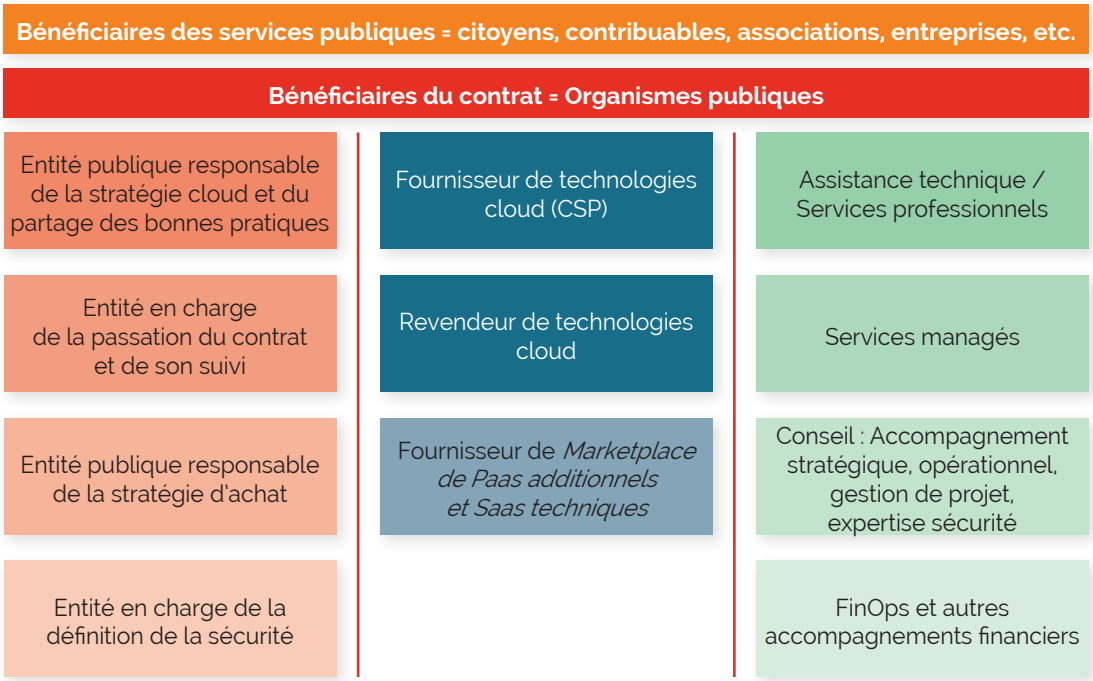


Schéma 1 - Rôles pour la mise en place de marchés publics de cloud

Un fournisseur de cloud n'est pas un intégrateur de systèmes ni un fournisseur de services managés. De nombreux acteurs public s'appuient sur un CSP pour leur infrastructure et délèguent à un intégrateur de systèmes ou à un fournisseur de services managé les tâches de planification, de migration et de gestion.

Si certains CSP offrent également la possibilité de bénéficier de services de conseils permettant à leurs clients de disposer d'avis d'experts et d'un accompagnement lors de la phase de migration de leur infrastructure, **il est une bonne pratique dans un marché de séparer les services de conseil / migration de la fourniture de prestation Cloud.**

Les responsabilités en matière de sécurité et de conformité sont partagées entre les CSP et les utilisateurs du cloud. Le niveau des responsabilités du CSP et de l'acteur public varie en fonction du modèle de déploiement du cloud et les acteurs publics doivent être conscients des responsabilités qui leur incombent dans chaque modèle.

Exemple : *dans un modèle IaaS, les clients maîtrisent la façon dont ils organisent et sécurisent leurs applications et données dans l'infrastructure. Les CSP, quant à eux, sont chargés de fournir les technologies sur une plateforme hautement sécurisée et contrôlée, ainsi que de proposer une vaste gamme de fonctionnalités de sécurité supplémentaires.*

Les utilisateurs de cloud doivent accéder au réseau de partenaires d'un CSP. Ces partenaires sont essentiels dans l'adhésion au cloud. Ils aident les acteurs publics à utiliser les outils du CSP et des logiciels tiers pour automatiser une grande part des tâches de rapport et de facturation impliquées dans la gestion de l'environnement cloud. Ce réseau doit être aussi diversifié que possible pour s'adapter à la diversité des profils de bénéficiaires et à la diversité de projets numériques.

Exemple : *un fournisseur de services managés peut aider à configurer pour le compte d'acteurs publics les capacités de contrôles fournis par un CSP pour répondre à leur conformité unique.*

3 DÉFINIR LE MODÈLE DE DISTRIBUTION ET LE PÉRIMÈTRE DES PRESTATIONS ASSOCIÉES

Nous décrivons ci-après des bonnes pratiques permettant de créer un cadre contractuel favorable au déploiement du cloud :

- L'acteur public, dans le cadre d'un appel d'offre d'envergure doit pouvoir choisir entre plusieurs CSP et pouvoir recourir à plusieurs CSP en même temps (modèle "multi-cloud"). Cette recommandation ne s'appliquant pas de manière systématique à des entités publiques de petite taille cherchant une solution pour des besoins limités.

- Les fournisseurs proposant des options de portabilité efficaces doivent être privilégiés. A contrario la captivité à un fournisseur doit être évitée.

- Un modèle de contrat mono-attributaire dans lequel un seul acteur du marché (type « cloud broker » ou revendeur) vend les technologies de plusieurs CSP n'est pas optimal. En effet, les marges de revente sont faibles puisque les prix publics sont les prix les plus optimisés. La revente seule est un modèle économique difficilement rentable pour le revendeur de CSP. Il cherche donc à ajouter à la revente de technologies cloud, des prestations d'accompagnement.

Or, imposer un acteur unique sur les services d'accompagnement pourrait nuire à l'adhésion des bénéficiaires. En effet, les champs d'application des technologies cloud sont bien trop vastes, depuis les services web au calcul scientifique en passant par les machines d'apprentissage automatique ou l'Internet des Objets.

Il est difficile de trouver un fournisseur de prestations d'accompagnement compétent dans la totalité des cas d'usage et adapté à tous les contextes d'organisations publiques.

> ***« Imposer un acteur unique sur les services d'accompagnement pourrait nuire à l'adhésion des bénéficiaires.***

Dans le cas où le modèle mono-attributaire via un revendeur paraîtrait inévitable, la politique d'achat devrait limiter le périmètre de prestations à la formation et l'assistance technique, et le rendre optionnel vis-à-vis de l'acquisition de technologies cloud. En parallèle, la gouvernance du marché devrait être dotée de mécanismes de contrôle de l'appétence du titulaire au développement commercial du marché tout au long de son exécution, ainsi que la valorisation des offres proposées par les différents CSP référencés par le revendeur, afin de ne pas privilégier un CSP par rapport à un autre dans le cadre de l'exécution du marché.

- Les procédures complexes pour la mise en œuvre d'un contrat cadre entraînent des lourdeurs nuisibles à la réactivité de traitement des demandes des bénéficiaires. Un accord-cadre imposant à chaque acteur public de repasser par des mécanismes d'appel d'offres supplémentaires (marchés subséquents) pour sélectionner son fournisseur risque de freiner le recours au cloud.

En droit français, le schéma contractuel mis en œuvre par les pouvoirs public anglais UK G-Cloud qui ne met pas en concurrence au moment de l'accord-cadre (tous les fournisseurs répondant aux critères sont qualifiés) ne peut pas être reproduit tel quel. En revanche, le mécanisme pour comparer agilement entre les fournisseurs qualifiés est lui reproductible en droit français et ce par l'émission de bons de commande selon des critères de sélection équitables et transparents[3], justifiables en cas de contrôle a posteriori. De plus, les règles françaises de la commande publique permettent toutefois d'envisager des méthodes de sélection agile :

- dans le cadre d'un marché avec une centrale d'achat en achat pour revente, avec un accord-cadre permettant autant que possible les échanges directs entre l'utilisateur des services cloud et les CSP et une liberté de choix de l'utilisateur ;
- dans le cadre d'un groupement de commande, avec un accord-cadre exécuté par marché subséquent sans remise en concurrence formalisée.

- Les prix doivent être transparents et homogènes pour faciliter la compréhension du marché et donc l'adhésion des bénéficiaires.

Deux options de structuration d'un marché de fourniture de technologies cloud offrent l'agilité la plus complète :

Option A - trois lots :

Lot 1 : fourniture de technologies cloud IaaS/PaaS et revendeurs (cases bleues foncées dans le Schéma 1) ;

Lot 2 : accès à une Marketplace de technologies tierces aux CSP de type PaaS-additionnel ou SaaS-technique[4] (case bleue claire) ;

Lot 3 : prestations de services autour du cloud telles qu'assistance technique / services professionnels, services managés, conseil, FinOps (cases vertes).

Option B - un lot + autres marchés :

consultation portant uniquement sur la fourniture de technologies cloud et l'assistance technique et utilisation d'autres marchés (existants ou très légèrement ultérieurs) pour les prestations de services et la *Marketplace*.

Variante de l'option B - un lot + ouverture à la déclaration de sous-traitants par le titulaire pour compléter l'offre en termes de services d'intégration sur les sujets très évolutifs techniquement comme le HPC, l'IA

[3] https://www.gov.uk/guidance/how-to-buy-digital-marketplace-services-fairly
[4] SaaS Technique : Solutions logicielles complémentaires au cloud et intégrables dans des architectures sur le cloud tels que solution d'analyse de logs, solution de filtrage, logiciel de bases de données, etc.

4 RENFORCER LES CRITÈRES DE SÉLECTION AU STADE DE LA CANDIDATURE

Une option qui permet l'évaluation de la qualification d'un CSP est d'abord d'opérer une analyse détaillée des dossiers de candidature sur la base de critères objectifs afin de ne retenir que les candidats les plus à même de se conformer aux enjeux du cloud.

Exemple : *le CSP devrait avoir des certifications de conformité x ou y, l'expérience de projets similaires, une présence locale, multi-locale ou mondiale, la présence dans l'analyse d'un tiers indépendant reconnu de l'industrie, etc.*

Le niveau de qualité de services attendu doit, par défaut, être élevé pour les CSP et les partenaires des CSP (Intégrateurs / MSP). Des standards de qualité et de sécurité fiables existent tels que ISO 27001, SOC 1, SOC 2, SOC 3, et sont largement adoptés par le marché. Quand ils existent, il convient également de solliciter des standards locaux. La qualité de service assure que les projets liés au cloud en France soient réalisés efficacement accélérant ainsi l'adoption par des retours d'expérience positifs dès les premières expériences.

La protection des données dans le cadre du Règlement Général sur la Protection des Données (RGPD) en vigueur en Europe est un élément clé à prendre en compte. Pour les services de cloud d'infrastructure, il est ainsi recommandé que les offres retenues soient conformes au « Code de conduite » CISPE sur la protection des données, ou d'autre codes qui pourraient être approuvés par le « European Data Protection Board » (EDPB) qui regroupe les autorités européennes de protection des données (ex. : CNIL…). Des codes développés en vue de permettre aux fournisseur d'infrastructure Cloud de démontrer leur conformité à ce règlement européen, et à leur client de bâtir leur propre conformité audit règlement.

Aussi, certains bénéficiaires contraints à des exigences réglementaires des plus strictes souhaiteront trouver des CSP qualifiés SecNumCloud et/ou agréés HDS.

Lors du choix d'un service, l'utilisateur doit être informé de la localisation dudit service, et le fournisseur devra donner la capacité au client de choisir le lieu de mise en œuvre dudit service explicitement (zone urbaine). La juridiction applicable est en élément un critère de choix à pouvoir prendre en compte. Un service non disponible sur le sol de l'Union Européenne ne doit pas être considéré dans le cadre d'un marché public. Toute restriction supplémentaire de localisation devra se faire en conformité avec le Règlement Européen sur la Libre Circulation des données non personnelles (Free Flow of non-personal Data[5]). Les offres étudiées seront quant à elles conformes à la doctrine de l'État au regard des régulations d'autres États pouvant éventuellement avoir une portée extraterritoriale (GDPR, CLOUD Act, E-evidence à venir…).

La disponibilité de sites de stockage des données présents à plusieurs endroits (distribués) est de nature à renforcer la fiabilité des services, et doivent pouvoir être considérés, notamment à des fins de plan de reprise d'activité (PRA).

Afin de permettre le passage le plus aisé possible d'un CSP à un autre à la fin du marché, ou au cours du marché dans le cadre d'un marché multi-attributaire, la stratégie de sortie (« exit stratégie ») devrait être documentée par le donneur d'ordre en amont. Pour faciliter ces stratégies de sortie, nous recommandons notamment à ce que les offres soient conforme à des Codes de Conduite sectoriels sur cette thématique, notamment ceux actuellement en développement prévu dans le cadre de l'Article 6 « Data Portability » du Règlement Européen sur la Libre Circulation des données.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1807

5 COMPARER LES OFFRES TECHNIQUES ÉQUITABLEMENT DANS LE CONTEXTE DU CLOUD

Les responsables de l'achat cloud doivent poser les bonnes questions afin d'obtenir les meilleures solutions. Une fois les besoins de l'administration recueillis, il convient de poser des questions ouvertes pour que chaque fournisseur puisse proposer son offre qui est, par nature, standard et industrialisée pour l'ensemble de ses clients.

Les stratégies d'achat de technologies cloud efficaces se concentrent sur les exigences de performances au niveau application.

Celles-ci donnent la priorité à la puissance de calcul et aux résultats, plutôt qu'au fait d'imposer les méthodes, l'infrastructure et le matériel permettant de répondre aux exigences de performances. La validation des technologies sous-jacentes pourrait être confiée aux organismes garants de la sécurité des systèmes d'information de l'État comme l'ANSSI.

Exemple : *Il est nécessaire de ne pas prescrire d'exigences liées à la configuration des racks, des serveurs, les distances entre les centres de données, etc.*

Grâce à ces bonnes pratiques d'évaluation des offres cloud, on peut réduire ou éviter des restrictions inutiles sur les technologies qu'ils utilisent, et garantissent l'accès aux solutions cloud les plus innovantes, sécurisées et économiques.

L'évaluation par des démonstrations ou la réalisation d'un prototype lors d'un atelier est une méthode qui a démontré son efficacité.

Cela permet en particulier, d'évaluer et de comparer l'élasticité réelle des technologies, de leur résilience, de leur performance et de l'accélération des déploiements, élasticité qui est consubstantielle de la définition du cloud, ou encore la faisabilité des stratégies de sortie.

6 COMPARER LES OFFRES FINANCIÈRES ÉQUITABLES DANS LE CONTEXTE DU CLOUD

Le modèle de comparaison des offres financières est un point crucial dans la passation de marché : là encore, comparer financièrement des offres de cloud implique une démarche différente de celle appliquée pour l'achat de technologies informatiques traditionnelles.

Il est important de construire une approche qui prend en compte les caractéristiques uniques du cloud. En effet :

- 1/ le catalogue des prix d'un CSP peut être de plusieurs dizaines de milliers de lignes,
- 2/ les modèles de tarification sont différents d'un fournisseur à un autre pour des intitulés d'unité d'œuvre a priori similaires,
- 3/ des technologies qui peuvent sembler similaires offrent des niveaux de service distincts avec ou sans support inclus.

Exemple : *La comparaison d'unités d'œuvre d'instances de calcul ou stockage n'est pas représentatif car chaque CSP construit des modèles incluant des technologies différentes dans leurs unités d'œuvre : résilience, durabilité, disponibilité, connectivité, stockage, sécurisation, support, etc.*

En conséquence, la démarche suivante est la plus appropriée à la comparaison financière de technologies cloud.

6.1 >> Comparaison des offres financières sur la base de scenarii

La comparaison des offres financières de technologies cloud évalués sur un cas d'usage défini prend en compte tous les aspects d'une solution : la configuration des technologies, les plages horaires des services, les services des partenaires, les remises standardisées des CSP disponibles.

Le processus d'évaluation peut alors intégrer les scenarii types qui correspondent à certains systèmes, applications ou usuels du secteur public :

Exemple : *Le traitement de volume élevé au moment de la déclaration de revenus, les notifications d'urgence telles que des avertissements d'inondation*

Les scenarii doivent être complets pour inclure l'étendue des technologies et services que l'acteur public est susceptible d'utiliser au cours du projet. De cette façon, l'acteur public est en mesure de comparer le coût total le plus optimisé dans son contexte.

Exemple : *certains leviers peuvent impacter significativement le coût total de possession : facturation (ou non) de l'usage du réseau, réservations d'instances, puissance de calcul et stockage supprimée la nuit, ajustement des ressources selon la nécessité de performance, de disponibilité, de temps d'accès, utilisation de ressources non utilisées du CSP et donc fortement remisées.*

6.2 >> Noter techniquement les scenarii

Il est également important de prendre en compte les avantages techniques, lors de la comparaison des offres.

Exemple : *Certains CSP proposent en standard un plan de continuité actif-actif-actif qui augmente significativement la sécurité des technologies. En comparaison, pour une sécurité équivalente, les autres CSP mettent en place une configuration x% plus chère.*

Une analyse holistique de la tarification prenant en compte les qualités techniques supplémentaires est cruciale pour évaluer les CSP. D'autres considérations peuvent être comparées, notamment liées à la sécurité et à la conformité.

Le fait de permettre aux CSP de proposer différents modèles de tarification permet aux organisations d'évaluer ces modèles en fonction de leurs propres besoins informatiques uniques, contrairement à une comparaison arbitraire de la tarification linéaire des « unités » de calcul ou de stockage.

Exemple : *Le prix de l'unité d'œuvre « stockage objet » de CSP-A est 0,025 € / Go. Le prix de CSP-B est de 0,10 € / Go. Dans une comparaison simple d'unité d'œuvre, CSP B est le plus avantageux.*

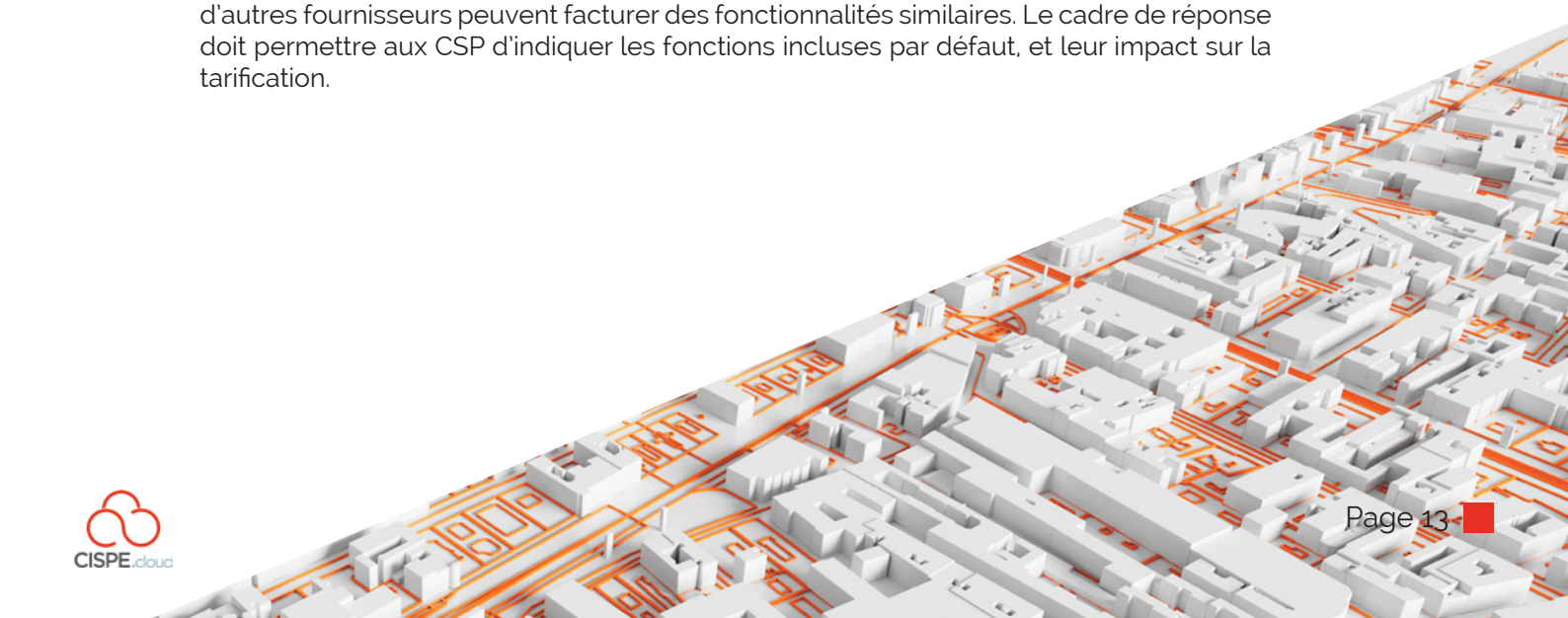
Pour autant, cette analyse ne prend pas en compte le nombre de copies de l'objet répliquées sur plusieurs sites ce qui permet de garantir la durabilité de l'objet dans le cloud, facteur de sécurité important.

En standard CSP-A en propose 3 et CSP-B une copie. L'offre de CSP-B doit donc être multiplié par 3 auquel il faut ajouter le coût d'une solution de réplication des objets pour être techniquement équivalente à l'offre de CSP-A.

D'autres aspects à prendre en compte sont les outils de gestion liés à la fourniture des technologies cloud. Certaines technologies, de sécurité notamment, peuvent être incluses gratuitement ou non.

Exemple : *Surveillance de la performance, protection DDoS, contrôle de l'accès aux technologies pour les utilisateurs, etc.*

Une évaluation technique devrait donc prendre ces technologies en compte, et le fait que d'autres fournisseurs peuvent facturer des fonctionnalités similaires. Le cadre de réponse doit permettre aux CSP d'indiquer les fonctions incluses par défaut, et leur impact sur la tarification.



7 CONTRACTUALISER EFFICACEMENT SUR LES PRIX

Pour établir un contrat de cloud qui tienne compte de l'évolutivité des besoins des bénéficiaires, les acteurs publics doivent conclure un contrat dont les modalités financières sont basées sur une logique de l'usage consommé.

De nombreuses solutions informatiques commerciales, y compris le cloud computing, s'appuient sur un modèle « à la demande », avec tarification à l'usage. Ce modèle économique réduit considérablement les coûts et stimule les rendements en garantissant que les consommateurs payent uniquement les ressources qu'ils utilisent réellement. Les acteurs publics payent ces ressources à des taux qui fluctuent en fonction de l'utilisation et des innovations. Les entités du secteur public perdent l'avantage de ce modèle lorsqu'elles établissent une tarification fixe des articles dans leurs contrats.

L'acteur public devrait par conséquent :

- (a) construire un modèle d'acquisition cloud pour les technologies à la demande, facturés à l'usage ;
- (b) fournir des conseils et des ressources aux agents en charge de la gouvernance du marché pour leur permettre d'effectuer le suivi des dépenses par rapport au budget et d'affecter des financements et des ressources supplémentaires selon les besoins (FinOps). Cette approche entraînera à terme une plus grande adoption du cloud et des investissements plus judicieux pour la modernisation de l'informatique dans le secteur public. Certaines bonnes pratiques de contractualisation financière permettent d'atteindre ces objectifs.

7.1 >> Prix variables

À la lumière du modèle de fourniture de services en réseau, qui permet d'offrir à très grande échelle des services standardisés à des millions de clients, il semble difficile qu'un CSP fournisse ses services à prix ferme, c'est-à-dire à un prix donné fixe sur toute la durée du marché. Le modèle d'acquisition cloud doit être flexible et permettre des variations du prix des services en fonction des prix du marché, généralement à la baisse. Cette approche est justifiée au regard de la nature dynamique et concurrentielle de la tarification du cloud, et elle soutient l'innovation et les réductions de prix. Cette flexibilité peut être obtenue en prévoyant dans les documents contractuels que le prix des prestations est variable en fonction du barème du titulaire du marché, ainsi que le permet la réglementation relative aux marchés publics.

7.2 Modèles de tarification multiples

Les sollicitations cloud doivent permettre aux CSP de proposer leurs propres modèles de tarification. Cela permet aux acteurs publics de sélectionner le modèle le plus adapté à leurs besoins uniques. Les sollicitations pour l'acquisition de solutions doivent pousser les soumissionnaires des intégrateurs de systèmes/cabinets de conseil à exploiter le modèle de tarification d'un CSP d'une façon optimale lorsqu'ils présentent la tarification dans leurs réponses aux sollicitations.

7.3 Services facturés à l'usage

L'intégration d'un modèle de service facturé à l'usage, dans lequel, à la fin de chaque mois, vous payez simplement ce que vous avez utilisé, est optimale pour les métriques d'utilisation et de ressources.

Les organisations du secteur public doivent également envisager une manière d'optimiser leurs dépenses liées au cloud en exploitant les offres de remises standardisées du CSP. Il s'agit, par exemple, de programmes de remise sous conditions de réservation de ressources sur plusieurs années.

8 PERMETTRE UNE NÉGOCIATION CONTRACTUELLE

Les technologies et les opérations sont par nature standardisées chez un fournisseur de service cloud, par conséquent, les conditions contractuelles le sont aussi. Il existe toutefois une capacité à ajuster marginalement ces contrats pour s'adapter aux contextes législatifs et réglementaires locaux.

Afin de pouvoir contractualiser dans le respect de la législation française, tout en s'appuyant sur les conditions contractuelles standardisées par l'acteur économique, il est recommandé :

- 1/ de solliciter auprès des candidats le contrat-type grand-compte secteur public et d'en prendre connaissance,
- 2/ de ne pas édicter des conditions contractuelles non adaptées au cloud dans l'appel d'offres et
- 3/ de prévoir un périmètre de négociation portant sur l'intégralité des clauses de la consultation et des propositions qui résulteront dans le marché sauf, évidemment, les clauses rendues obligatoires par la loi ou par nature intrinsèquement liées à la nature des services de cloud public.

Le périmètre de responsabilité partagée inhérent au cloud (cf. point 2) doit se retrouver dans les clauses du contrat.

Exemple : *Le prestataire doit donner la possibilité de localiser ses données et de fournir des outils pour s'assurer que le choix des localisations est limité mais il est de la responsabilité de l'acteur public ou d'un partenaire d'activer ces outils sur les données concernées.*

Exemple : *Dans le cadre du RGPD, un service d'Infrastructure Cloud, le prestataire est un responsable de traitement. Le prestataire devra ainsi assister son client (contrôleur) afin de répondre à ses propres obligations au sens du RGPD, en respectant par exemple des bonnes pratiques sectorielles d'un Code de Conduite.*

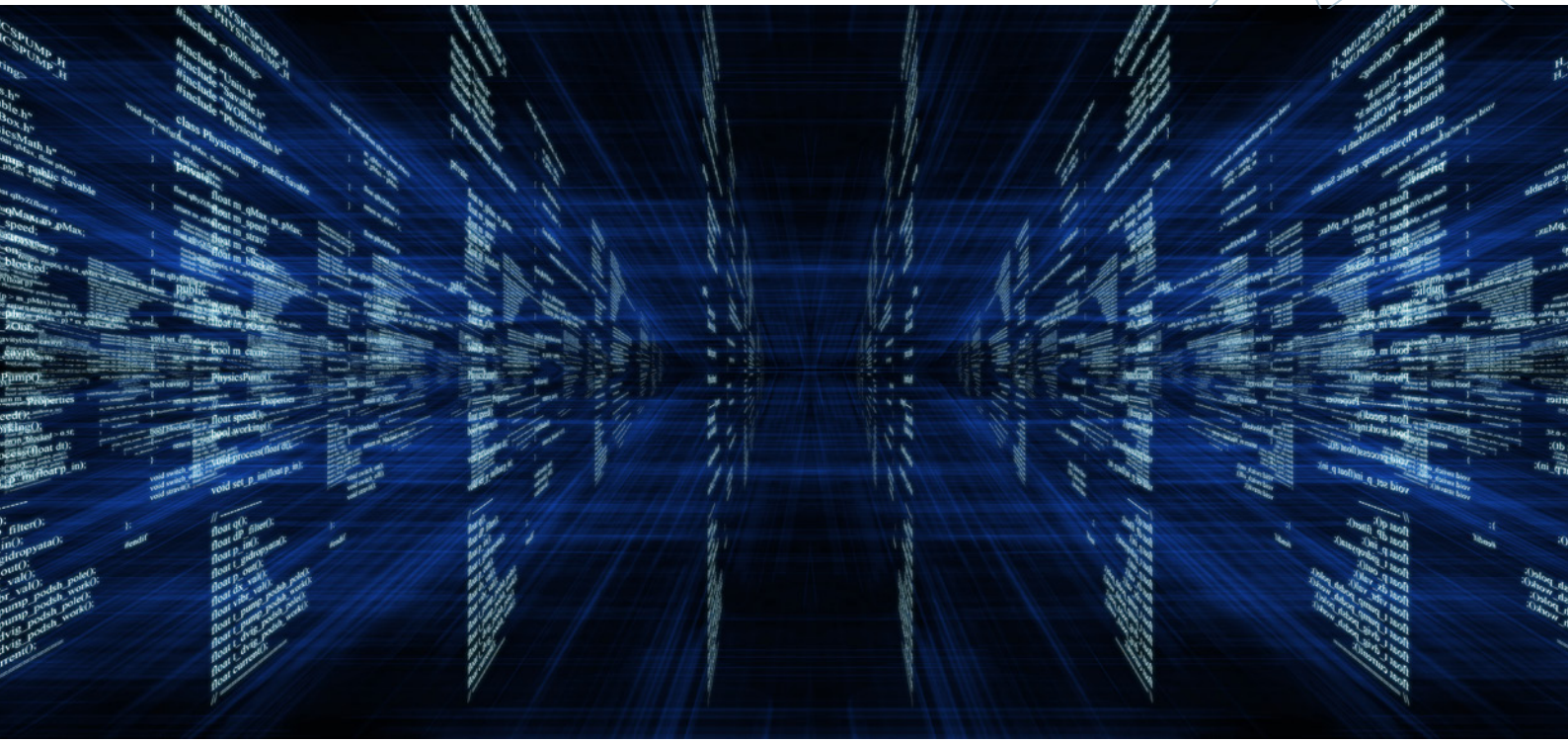
9 ACCOMPAGNER L'ACCULTURATION AU CLOUD

Il est essentiel de bien comprendre que le cloud est généralement utilisé dans un modèle de type DevOps agile, dans lequel l'utilisateur final modifie et rationalise en permanence l'architecture.

Cela implique de donner aux utilisateurs finaux la possibilité d'accéder à toutes les technologies, tout en mettant en place des contrôles a priori et a posteriori pour qu'ils se conforment aux pratiques de sécurité et de dépenses internes.

C'est pourquoi, il est essentiel que les bénéficiaires soient accompagnés dans leur montée en compétences sur la dimension de gouvernance dans un environnement cloud afin d'en tirer le meilleur parti.

Chaque bénéficiaire gagnera ainsi en autonomie dans la gestion des fonctions d'achat, de service, de localisation, de réversibilité ou encore de sécurité de leur projets digitaux sur le cloud.



10 AJUSTER LES CONDITIONS CONTRACTUELLES ADMINISTRATIVES

Il est compréhensible que les termes des clauses générales administratives actuelles régissant l'acquisition de services relatifs aux technologies de l'information (ex. : CCAG TIC en France) soient mal adaptées à la fourniture de technologies cloud qui est un domaine d'activité récent. Certaines dispositions sont en effet inapplicables à l'objet même du cloud. À ce titre, des dérogations et compléments essentiels sont à prévoir (en France, dans le cahier des clauses administratives particulières CCAP). Nous détaillons les dispositions à prévoir dans un tableau d'analyse exhaustif fourni en annexe.

Les ajustements intégrés peuvent facilement s'inspirer des conditions générales définies par les CSP. En effet, les Conditions Générales d'un CSP garantissent que les acteurs publics profitent de processus d'achat flexible pour tirer tous les avantages du cloud.

Ces conditions générales sont consolidées au niveau mondial et fonctionnent à très grande échelle, favorisant ainsi l'innovation et réduisant les coûts. Ce point a été démontré dans la stratégie d'informatique en nuage de la Norvège :

Exemple : *L'achat de cloud diffère à de nombreux égards des processus d'achat traditionnels dans le secteur public. Les acteurs publics peuvent avoir du mal à choisir le bon contrat. Les technologies en nuage sont souvent vendues selon des conditions générales qui s'appliquent à tous les clients. Difi [Agence de gestion publique et d'administration en ligne] a révisé les conditions générales standard du gouvernement (SSA) en 2015 ; ces nouveaux accords sont mieux adaptés aux technologies de cloud computing que les anciens, qui établissaient une distinction claire entre logiciel et fonctionnement. Les nouveaux accords permettent d'inclure les conditions générales standard du fournisseur de technologies. Ils peuvent donc être utilisés pour acheter un accès à des systèmes standard dans le cloud. Le SSA est ensuite complété avec le contrat de service standard du fournisseur de technologies et, le cas échéant, le contrat de traitement de données basé sur le modèle fourni par l'autorité de protection des données norvégienne.*

D'autre part, les acteurs publics doivent prévoir l'évolution des Conditions Générales afin de bénéficier des améliorations de technologies qui prévalent dans le cloud. Des restrictions inutiles ou des exigences en matière de consentement préalable au changement peuvent limiter la capacité des fournisseurs d'améliorer leur offre et des acteurs publics de tirer parti des modifications fréquentes apportées aux technologies innovantes et sont contraires au modèle cloud public en constante évolution.

En fin de compte, la création de Conditions Générales statiques ou spécifiques aux technologies informatiques traditionnelles ne permettra pas la flexibilité ou l'évolutivité alors que, justement, le cloud est une technologie dynamique et en évolution rapide. Ceci entraînera des renégociations et adaptations, au cas par cas, lors de la mise en place opérationnelle, et ajoutera des freins au projet et donc à l'adhésion des bénéficiaires au cloud.

10 CLÉS pour l'Acheteur Public de Cloud

GUIDE PRATIQUE

#NATIONCLOUD

ANNEXES

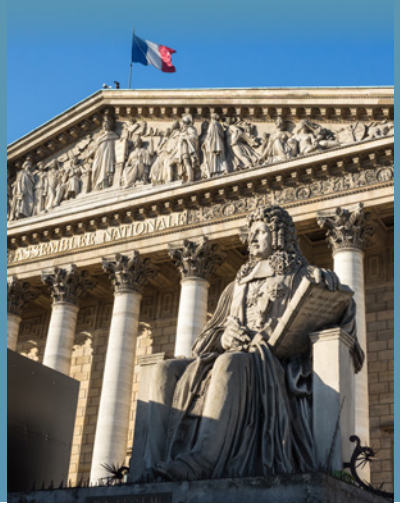
France - CCAG-TIC - Dérogations, compléments et articles inapplicables aux marchés ayant pour objet la fourniture de services de cloud

La présente annexe comporte un tableau d'analyse des dérogations et compléments essentiels au CCAG-TIC français à prévoir dans les cahiers des clauses administratives particulières (CCAP) des accords-cadres ayant pour objet la fourniture de services de cloud aux administrations françaises.

Elle comporte également une liste des dispositions du CCAG-TIC qui ne seront pas applicables aux accords-cadres précités, dans la mesure où elles sont inadaptées à l'objet-même du cloud.

Il convient de préciser que l'expression « bénéficiaires » est employée ci-dessous dans le contexte de l'attribution d'accords-cadres ayant plusieurs entités publiques comme bénéficiaires du marché.

Par ailleurs, la présente annexe vise l'hypothèse de marchés ayant pour objet la fourniture de services de type « IaaS » et « PaaS ».



Dérogations et compléments au CCAG-TIC

Dispositions du CCAG-TIC	Nature de la modification	Incompatibilités avec les principes de fonctionnement et/ou le modèle commercial du cloud Propositions de dérogation et/ou compléments essentiels
Article 2 - Définitions	Complément	L'article 2 ne comporte pas de définition des services de cloud, en particulier des services de type « IaaS » et « PaaS ». Or, ces derniers constituent l'objet même des accords-cadres envisagés dans le cadre de la présente annexe, et leur définition peut varier significativement en fonction des différents prestataires de services de cloud. Il conviendrait donc de compléter les dispositions du CCAG-TIC en incluant une définition standard des services de type « IaaS » et « PaaS » dans le CCAP. À titre d'exemple, il pourrait être envisageable de s'inspirer de définitions qui font autorité dans l'industrie du cloud, telles que celles élaborées par le NIST (SP 800-145) ou la norme ISO/IEC 17788:2014. Les services « IaaS », au sens du NIST, renvoient à la *« mise à disposition à un consommateur du traitement, du stockage, des réseaux et d'autres ressources informatiques fondamentales, alors que le consommateur conserve la faculté de mettre en œuvre et d'exploiter des logiciels de son choix, qui peuvent inclure des systèmes d'exploitation et des applications. Le consommateur ne gère ni ne contrôle l'infrastructure cloud mais exerce le contrôle des systèmes d'exploitation, du stockage et des applications mises en œuvre, et exerce éventuellement un contrôle limité sur la sélection de certains composants réseau (par exemple les pare-feu hôtes) ».* Les services « PaaS », au sens du NIST, renvoient à *« mise à disposition à un consommateur de mettre en œuvre sur l'infrastructure cloud des applications qu'ils ont créées ou acquises, en utilisant des langages de programmation, des bibliothèques, des services et des outils fournis par le fournisseur. Le consommateur ne gère ni ne contrôle l'infrastructure cloud, en ce inclus les réseaux, serveurs, systèmes d'exploitation et le stockage, mais exerce un contrôle sur les applications mises en œuvre, et éventuellement sur les paramètres de configuration de leur environnement d'hébergement ».* La norme ISO/IEC 17788:2014 définit les services « IaaS » comme une *« catégorie de services de cloud dans laquelle le type de capacités offertes au consommateur de services de cloud sont des capacités de type infrastructure ».* La norme ISO/IEC 17788:2014 définit les services « PaaS » comme une *« catégorie de services de cloud dans laquelle le type de capacités offertes au consommateur de services de cloud sont des capacités de type plateforme ».*
Article 5.2 - Protection des données à caractère personnel	Dérogation	L'article 5.2 du CCAG-TIC s'applique à toute collecte ou traitement de données à caractère personnel auxquelles le titulaire a accès pour les besoins de l'exécution du marché. A l'heure du RGPD, le contenu de l'article 5.2 paraît largement insuffisant et inadapté. Le vocabulaire utilisé est très éloigné de la réglementation applicable (RGPD et Loi Informatique et Libertés modifiée par la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles), et les quelques sujets évoqués confirment le caractère obsolète de la clause :

1. L'article 5.2.1 lie l'obligation de conformité à la réglementation de protection des données à l'accès aux données pour les besoins de l'exécution du marché

Ce critère d'application est trop restrictif, et il devrait être dérogé à cet article dans le CCAP pour intégrer les principes suivants :

Selon la conception du RGPD, tous les acteurs sont responsables de la conformité, y compris les sous-traitants de données personnelles qui ont désormais des obligations directes et sont susceptibles d'être sanctionnés en cas de manquement. De plus, les problématiques de protection des données personnelles soulevées lors de l'analyse des prestations de cloud ont souvent été développées autour des sujets de délocalisation des données et de mutualisation dans des environnements partagés, faisant craindre des risques d'atteinte à la confidentialité des données. Il est donc important, pour tenir compte de ces craintes et sécuriser les données du pouvoir adjudicateur ayant recours à des prestations de cloud, de rappeler que responsable de traitement et sous-traitant se conforment en tous points à la réglementation applicable.

Cet article devrait aussi donner la possibilité aux parties de préciser leur qualité : responsable de traitement, sous-traitant, ou responsable de traitement conjoint, et de renvoyer au détail du traitement effectué dans le cadre de la commande publique. En matière de cloud computing, le sujet de la répartition des rôles est complexe. Dès 2012 la CNIL publiait des recommandations pour les entreprises utilisant des services de cloud computing (*https://www.cnil.fr/fr/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services*) suite à une consultation publique sur le cloud, dans lesquelles elle insistait notamment sur le besoin de s'arrêter sur les qualifications pour déterminer le régime applicable, et de vérifier si le prestataire de services cloud était un sous-traitant ou un responsable de traitement conjoint. Il fait aujourd'hui moins de débats qu'un prestataire de services cloud est un sous-traitant de données personnelles..

L'article 5.2.2 se focalise sur les impacts d'un changement de réglementation

Le RGPD étant désormais maintenant pleinement applicable, le besoin est plutôt d'organiser le contrat public de telle façon que le pouvoir adjudicateur et le titulaire soient en mesure d'en respecter tous les termes. Le CCAP devra intégrer les éléments suivants :

Le champ de la réglementation applicable doit être précisé. Aujourd'hui, un tel article devrait prévoir que le titulaire d'un marché public et le pouvoir adjudicateur doivent s'engager à respecter la réglementation applicable à la protection des données à caractère personnel, y compris la loi française relative à la protection des données personnelles ainsi que, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. En France, la Loi Informatique et Libertés a été modifiée par la Loi du 20 juin 2018, et même si la Commission Européenne et les différentes autorités européennes continuent d'émettre des

recommandations sur l'interprétation du RGPD qui pourraient modifier en cours d'exécution du marché la portée de certaines obligations de protection des données personnelles, les changements du cadre législatif ne devraient pas être significatifs. En revanche, il serait pertinent de viser les recommandations et référentiels applicables par industrie (par exemple SecNumCloud) ou encore des normes sectorielles (par exemple ISO/IEC 17788 et ISO/IEC 17789 applicables au cloud computing), pour permettre d'appréhender le sujet de la protection des données dans toute sa dimension pratique et opérationnelle.

L'obligation de donner des instructions et autorisations spécifiques au sous-traitant de données personnelles définie par l'article 28 du RGPD s'applique à l'acheteur public. Selon le paragraphe 2 de l'article 28 du RGPD, l'acheteur public doit donner au titulaire du marché son autorisation écrite préalable, spécifique ou générale, au recrutement d'un sous-traitant au contrat lorsque ce dernier est chargé de traitements de données à caractère personnel. Pour faciliter cette demande d'autorisation, la Direction des affaires juridiques (DAJ) de Bercy a collaboré avec la CNIL afin de mettre à jour le formulaire DC4 relatif à la déclaration de sous-traitance. Ce dernier intègre désormais une rubrique « sous-traitance de traitement de données à caractère personnel ». Le CCAG-TIC ne tient pas encore compte de ce changement, et, pour se conformer au paragraphe 4 du même article 28 du RGPD, il devrait être dérogé à l'article 5.2.2 dans le CCAP pour décrire les instructions données par le pouvoir adjudicateur au titulaire du marché pour le traitement de données personnelles, tout en ménageant un mécanisme dans le cadre duquel les parties peuvent travailler ensemble à la définition des conditions de traitement des données dans le cadre du marché. Ce travail peut être effectué à partir de la documentation du fournisseur, y compris de son modèle de « contrat de traitement » conforme à l'article 28 RGPD, qui embarque nécessairement des spécificités liées aux services qu'il fournit qu'un document général ne peut pas saisir. À défaut, les prestataires de services en mode cloud se trouvent trop souvent bloqués par un cadre de traitement trop rigide et inadapté. Par exemple si l'acheteur public impose un droit d'audit très large donnant le droit d'accéder à des infrastructures d'hébergement sécurisées pour vérifier les conditions de traitement des données personnelles, le prestataire risque de ne pas pouvoir respecter certains engagements de sécurité liés à ces infrastructures. À propos de sécurité, il est impératif que des règles de sécurité des données et des infrastructures adaptées à l'environnement cloud (en terme notamment de sauvegarde, accessibilité, disponibilité, portabilité, sécurité de l'hébergement, évolutivité) soient intégrées dans le cadre contractuel.

2. L'article 5.2.3 met l'accent sur les déclarations et autorisations CNIL

Les déclarations CNIL ont disparu depuis le 25 mai 2018, date d'entrée en application du RGPD et les autorisations préalables de la CNIL sont réduites à des hypothèses limitées (par exemple, en cas de transfert de données vers un pays situé en dehors de l'Union Européenne et d'une utilisation de clauses contractuelles ad hoc pour encadrer le transfert). Le RGPD promeut à

		présent une logique d'« *accountability* », ou « obligation de rendre compte », qui oblige les responsables de traitement et sous-traitants à documenter leur démarche de conformité. Dans le cadre de services cloud, cette obligation de rendre compte prend une importance toute particulière s'agissant de l'obligation d'encadrer les potentiels transferts de données personnelles en dehors de l'Union Européenne. Un fournisseur de services en mode cloud peut faire appel à différents sous-traitants, par exemple à des fins de maintenance, qui sont situés en dehors de l'Union Européenne, si des mécanismes de sécurisation des transferts conformes à la réglementation applicables (comme des clauses contractuelles types adoptées par la Commission Européenne) sont mis en place par le titulaire. Il conviendrait donc de déroger à cet article 5.2.3 dans le CCAP pour mettre l'obligation d' « *accountability* » à la charge des deux parties, et pour rappeler les règles applicables aux transferts de données.
Article 10 - Prix et règlement	Dérogation	a) L'article 10.1.1 du CCAG-TIC prévoit, à titre de règle générale, que les prix du marché sont fermes. Or, un prix invariable sur toute la durée du marché ne semble pas adapté aux principes de fonctionnement et au modèle commercial des services de cloud, dès lors que ces derniers ne constituent pas des prestations courantes. En outre, un prix ferme serait d'autant moins pertinent si la durée du marché venait à être longue. Enfin, les modalités de mise en œuvre de l'actualisation, qui ne peut être effectuée qu'une seule fois et selon des conditions restrictives (lorsqu'un délai de plus de trois mois s'est écoulé entre la date à laquelle le candidat retenu avait fixé son prix dans l'offre et la date du début d'exécution des prestations), ne semblent pas de nature à permettre une modification du prix permettant de refléter les variations économiques susceptibles d'affecter l'industrie des services de cloud. Il conviendrait donc de déroger aux dispositions du CCAG-TIC en prévoyant que les prix du marché sont révisables, par exemple par alignement à des prix publics (qui ont tendance à baisser dans le cloud).
Article 23 - Installation et mise en ordre de marche	Dérogation	L'article 23, dans la mesure où il vise l'installation et la mise en ordre de marche du « *matériel* » et des « *logiciels* », n'est pas pertinent pour les services de cloud en mode IaaS et PaaS, les personnes publiques pouvant accéder sans délai à ces services disponibles « sur étagère ». En outre, dans l'environnement cloud, l'installation et la mise en ordre de marche nécessitent que l'acteur public se conforme aux prérequis d'exploitation distante du service et aux recommandations liées à la configuration, qui sont fournies par les prestataires concernés. b) En revanche, s'agissant d'un marché de cloud les notions d'installation et de mise en ordre de marche s'accordent à la mise à disposition aux bénéficiaires du portail de présentation des services de cloud par l'attributaire du marché. Il conviendrait toutefois de déroger aux dispositions du CCAG-TIC, en prévoyant dans le CCAP que l'installation et la mise en ordre de marche du portail interviendront dans un délai donné (par exemple, un certain nombre de jours à compter de la notification du marché).

Article 26 - Vérifications qualitatives Article 27 - Décisions après vérifications	Dérogation	De manière générale, une procédure de vérification d'aptitude (articles 26.2.1. et 27.2.1) et /ou de vérification de service régulier (VSR - articles 26.2.2 et 27.2.2.) ne s'accorde pas avec la fourniture de services de cloud, dans la mesure où ces services sont standards, disponibles « sur étagère » et immédiatement mis à disposition des utilisateurs, en ligne. Il conviendrait donc de déroger aux dispositions du CCAG-TIC, en excluant dans le CCAP toute procédure de recette. Le CCAP pourrait prévoir qu'en l'absence d'une telle procédure, les bénéficiaires pourront procéder, à leur discrétion au contrôle de la conformité et de la qualité des services fournis. En outre, les documents contractuels devront prévoir des engagements de qualité de service (ou «SLA» en anglais) de la part des fournisseurs de cloud, recouvrant notamment la pérennité des données et la disponibilité des services. Le contrôle de la conformité et de la qualité des services fournis sera effectué par rapport à ces engagements. Il pourrait être envisagé que les engagements de qualité de service soient définis dans le cahier des clauses techniques particulières (CCTP), par référence aux SLA des fournisseurs de cloud. Cette référence directe aux SLA des fournisseurs de cloud est justifiée par le fait que les services de cloud sont standard, fournis à l'échelle mondiale et de façon transverse. Dès lors, il n'est pas envisageable de définir des niveaux de disponibilité des services et de pérennité des données spécifiques dans le cadre d'un cloud public : ces niveaux seront les mêmes que ceux garantis à tous les usagers des services de cloud proposés par les fournisseurs.
Article 28 - Réception, ajournement, réfaction et rejet	Dérogation	Les notions d'ajournement, réfaction et rejet, telles que définies à l'article 28, ne s'accordent pas avec le modèle de fourniture de services de cloud, dès lors que ces services sont standards et immédiatement mis à disposition des consommateurs, en ligne. Il conviendrait le cas échéant de déroger au CCAG-TIC en prévoyant dans le CCAP qu'au terme des contrôles inopinés effectués par les bénéficiaires, de la conformité et de la qualité des services fournis, les fournisseurs devront mettre les services en conformité par rapport aux documents contractuels, à leurs propres frais et charges, dans un délai défini par le CCAP.
Articles 16 - Lieu d'exécution Articles 22 - Surveillance en usine	Dérogation	Les articles 16 et 22 ne sont pas entièrement adaptés à la fourniture de services de cloud, dans la mesure où les notions de « lieu d'exécution des prestations » et d'« usine » ne sont pas compatibles avec celle de centre de données. Elles pourraient dès lors causer des difficultés d'interprétation. Surtout, les visites et audits sur site ne sont pas adaptés à la fourniture de services de cloud, eu égard aux conditions de sécurité particulièrement strictes applicables aux centres de données des fournisseurs de services de cloud et à leur exploitation (et compte tenu du fait que les fournisseurs de cloud sont responsables de la sécurité des centres de données). Il convient d'ailleurs de préciser que ces visites et audits des centres de données ne sont effectués que par des tiers, dans le cadre de certifications attribuées aux fournisseurs de services de cloud (par exemple SecNumCloud, HADS, SOC 1/2/3, ISO 27001/27017/27018). Il conviendrait donc de déroger aux dispositions du CCAG-TIC, en prévoyant dans le CCAP que les bénéficiaires et le pouvoir

		adjudicateur pourront discuter et s'accorder avec le CSP sur les aux dates et fréquences de ces audits, portant sur les seuls comptes et éléments financiers relatifs à l'exécution des services et au respect des engagements contractuels du titulaire. Les conditions contractuelles pourront également prévoir un audit des services en ligne, par un auditeur externe et indépendant dont l'identité serait indiquée au CSP, lui permettant ainsi d'exercer un droit d'objection en cas de conflit d'intérêt par exemple.
Article 31 - Définitions	Dérogation	L'article 31.1 comporte une définition qui, dans la mesure où elle renvoie à la notion de *« matériels »*, n'est pas adaptée aux services de cloud. Il conviendrait donc de déroger aux dispositions du CCAG-TIC en incluant dans le CCAP une définition de la maintenance qui renvoie aux services de cloud.
Articles 36, 37 et 38 - Propriété intellectuelle	Dérogation	Les articles 36, 37 et 38 du CCAG-TIC détaillent les règles de propriété intellectuelle applicables (i) aux connaissances antérieures, (ii) aux logiciels standards, et (iii) aux résultats du marché. Si la protection des connaissances antérieures (article 36) peut être aménagée pour être appliquée au contexte du cloud, la concession de licence sur les logiciels standards (article 37) et la concession ou la cession de droits de propriété intellectuelle sur le résultat des services (article 38) ne sont pas du tout adaptés. En matière de IaaS et de PaaS, le fournisseur ne met pas à disposition un logiciel, comme dans le SaaS. Il n'y a donc pas de licence de « logiciel standard ». De plus, avec le cloud, les principes de « propriété », dont on concède une licence d'utilisation ou que l'on transfère, s'effacent au profit de la définition de droits d'utilisation de services. Les parties devront néanmoins rappeler l'étendue de leurs droits de propriété intellectuelle respectifs sur les éléments devant être utilisés dans le cadre du marché (les connaissances antérieures). Le fournisseur de services cloud devra rester propriétaire des éléments constitutifs du IaaS et du PaaS protégé par des droits de propriété intellectuelle, conformément à l'esprit de l'article 36.1 du CCAG-TIC sur les connaissances antérieures, mais comme il n'y aura pas de situations où ces connaissances antérieures pourront être « incorporées » dans les résultats du marché, l'ensemble des paragraphes de l'article 36, qui mentionnent cette hypothèse, il conviendrait de déroger à l'article 36 dans le CCAP pour redéfinir son champ d'application et le rendre applicable à des services en mode cloud. En principe, le fournisseur de services cloud reste propriétaire de son infrastructure ou de la plateforme objet des droits de propriété intellectuelle, ou est le seul titulaire des accords qui lui permettent de les héberger, s'il n'assure pas lui-même cet hébergement. La définition de l'étendue des droits d'utilisation du IaaS et du PaaS reposera alors sur la description des fonctionnalités et prestations couvertes. Il ne s'agira pas, comme dans le cadre d'une licence classique, de permettre à l'acteur public de « reproduire, représenter, exploiter, adapter, etc. », et autres droits qui sont généralement décrits dans des clauses de licence en vue d'assurer leur conformité au Code de la Propriété Intellectuelle français. De même, la durée d'utilisation accordée par

		le fournisseur de services en mode cloud ne pourra pas correspondre à « la durée légale des droits d'auteur » visée par l'article 37.1 du CCAG-TIC, elle correspondra plutôt à la durée d'abonnement définie avec le pouvoir adjudicateur. Les dispositions sur les codes sources de l'article 37.2 sont également inadaptées à des services portant sur une infrastructure ou une plateforme. Quant à la garantie de jouissance paisible de l'article 37.3.4, elle pourrait s'appliquer, sous réserve d'être adaptée pour s'appliquer plus précisément aux connaissances antérieures (et ne plus s'appliquer aux logiciels standards), et se concentrer sur l'indemnisation de l'acheteur public si des tiers venaient revendiquer des droits de propriété intellectuelle sur les éléments constitutifs du IaaS ou du PaaS. Il conviendrait donc de déroger à l'article 37 dans le CCAP pour retirer la licence de logiciels standards et couvrir plus spécifiquement le sujet de la jouissance paisible. Les dispositions de l'article 38 sur les résultats ne pourront pas s'appliquer directement à l'objet des services cloud, qui ne correspondent pas à des services de développement, et ne produisent donc pas de « résultats ». Néanmoins, si les services requis par le pouvoir adjudicateur vont au-delà du pur PaaS ou IaaS, et nécessitent par exemple de développer des interfaces permettant d'intégrer le service dans l'environnement de l'acteur public, il conviendra de définir les modalités d'utilisation de ces développements. Dans un environnement PaaS ou IaaS, les interfaces ou autres développements devraient être normalisés, et publiés par le fournisseur de service cloud pour tout client. Effectuer des développements spécifiques pour un seul client n'est pas compatible avec la logique même du cloud. Ces développements « normalisés » devraient être proposés en licence, toute cession étant exclue, car totalement incompatible avec l'esprit du cloud. Les fournisseurs de services cloud doivent pouvoir continuer d'innover en se reposant sur leurs développements. Il conviendrait donc de déroger à l'article 38 dans le CCAP pour préciser le régime applicable, le cas échéant, à des développements effectués par le titulaire en marge de la pure fourniture du PaaS ou du IaaS.
Article 13. - Délai d'exécution	Dérogation	La notion de *« délai d'exécution »* des prestations, prévue à l'article 13., n'est pas adaptée aux services de cloud en mode IaaS ou PaaS, dans le cadre desquels l'exécution des services est quasi instantanée et consiste en réalité en une fourniture d'accès au cloud. La notion d'engagement de qualité de service (ou «SLA» en anglais), recouvrant notamment la pérennité des données et la disponibilité des services, est plus appropriée. Il conviendrait donc de déroger aux dispositions du CCAG-TIC, en prévoyant de substituer dans le CCAP la notion de *« délai d'exécution »* à celle d'engagement de qualité de service. Ces engagements de qualité de service seraient définis dans le cahier des clauses techniques particulières (CCTP) par renvoi aux SLA des fournisseurs de services de cloud, pour les raisons évoquées ci-dessus *(cf. commentaires sur les Articles 26 et 27)*.
Article 14 - Pénalités	Dérogation	L'article 14 n'est globalement pas adapté à la prestation de services de cloud. En particulier, la notion de délai d'exécution des prestations, incluse dans la formule de calcul des pénalités de retard prévue à l'article 14.1.1., n'est pas adaptée au fonctionnement du cloud (voir les remarques ci-dessus).

		Il conviendrait donc de déroger aux dispositions du CCAG-TIC en prévoyant dans le CCAP des pénalités pour non-respect des engagements de qualité de service. Il pourrait être envisagé de prévoir que ces pénalités seront appliquées conformément aux conditions définies par les SLA des fournisseurs de services de cloud. En règle générale, les SLA prévoient, en fonction du pourcentage de disponibilité mensuelle des services, que les fournisseurs mettront à disposition des bénéficiaires des crédits de services utilisable par les bénéficiaires dans la période de facturation suivante. Les SLA prévoient également toutes les dispositions relatives à la présentation de la demande de paiement par les consommateurs des services. Ces pénalités, eu égard aux risques encourus par les fournisseurs de services de cloud (notamment de sécurité et de pertes de données), seraient plafonnées, suivant les conditions définies par les SLA, et représenteraient le recours exclusif en cas d'indisponibilité des services concernés.
Article 8 - Réparation des dommages	Complément / Dérogation	a) L'article 8 ne comporte pas de clause limitative de responsabilité du titulaire du marché. Les commentaires sous cet article envisagent toutefois la possibilité, *« en cas de risque hors de proportion avec le montant du marché », de « prévoir au CCAP des dispositions particulières pour un plafonnement éventuel des garanties »*. Au cas d'espèce, les risques encourus par le titulaire du marché seront importants par rapport au montant du contrat (du fait notamment de l'engagement potentiel de sa responsabilité en cas de perte de données publiques). En outre, il convient de mentionner ici que la sécurité du cloud obéit à un modèle de responsabilité partagée. Alors que les fournisseurs de services cloud sont responsables de la sécurité des infrastructures et des données, les bénéficiaires de ces services sont quant à eux responsables de l'usage qu'ils en font. Ils sont également responsables de la conception et de l'architecture des applications et des solutions rendues opérationnelles grâce au cloud. Eu égard à ce modèle de responsabilité partagée, il semble logique d'inclure une limitation de responsabilité des fournisseurs de service de cloud. Il conviendrait donc de compléter les dispositions du CCAG-TIC en incluant dans le CCAP une clause limitative de responsabilité des fournisseurs de services de cloud corrélée au montant du contrat. La jurisprudence administrative admet que le CCAP annexé au marché comporte une clause venant limiter (et non exclure) la responsabilité du titulaire du marché, qui, pour être opposable au pouvoir adjudicateur, doit être expressément écrite. En toute hypothèse, une telle clause limitative de responsabilité, si elle venait à être incluse dans le CCAP, pourrait être écartée en cas de faute lourde des fournisseurs de services de cloud. b) L'article 8.1 prévoit que les dommages de toute nature causés au pouvoir adjudicateur par le titulaire, du fait de l'exécution du marché, sont à la charge du titulaire. Eu égard au modèle de responsabilité partagée évoqué ci-dessus, il conviendrait de compléter les dispositions du CCAG-TIC, en précisant dans le CCAP que seuls les dommages directs, matériels et immatériels, causés aux bénéficiaires par les fournisseurs de services de cloud seront à la charge de ces derniers.

Chapitre 8 - Résiliation	Complément	Les articles 39 à 43 prévoient les hypothèses dans lesquelles la personne publique peut résilier le marché. En revanche, le CCAG-TIC ne prévoit pas de dispositions permettant au cocontractant de la personne publique de suspendre l'exécution du contrat. Il apparaît, au cas présent, nécessaire de prévoir que les fournisseurs de services de cloud puissent suspendre temporairement l'accès des bénéficiaires aux services dans le cas où la sécurité du cloud serait compromise (que l'atteinte provienne des bénéficiaires eux-mêmes ou non). Les cas de suspension définitive ou de dépréciation du service doivent également être prévus. La jurisprudence administrative (CE, 8 octobre 2014, Société Grencke Location, req. n°370.644) permet désormais de prévoir dans un contrat qui n'a pas pour objet l'exécution même du service public les conditions auxquelles le cocontractant de la personne publique peut résilier le contrat, en cas de méconnaissance par cette dernière de ses obligations contractuelles. Le cas échéant, la résiliation ne peut intervenir sans que le cocontractant ait mis la personne publique à même, au préalable, de s'opposer à la rupture des relations contractuelles pour un motif d'intérêt général. Cette jurisprudence autorisant la résiliation unilatérale (sous conditions) du marché par le cocontractant de l'administration peut être interprétée comme permettant au cocontractant, a fortiori, de suspendre temporairement l'exécution des prestations contractuelles (parce que la personne publique a méconnu ses obligations contractuelles ou pour un autre motif). Il conviendrait donc de compléter les dispositions du CCAG-TIC en prévoyant dans le CCAP la possibilité pour les fournisseurs de services cloud de suspendre temporairement l'accès des bénéficiaires aux services, dans le cas où la sécurité du cloud serait compromise. Le CCAP prévoirait que la suspension temporaire ne pourrait être mise en œuvre sans que le titulaire ait, au préalable, mis les bénéficiaires à même de s'y opposer pour un motif d'intérêt général (conformément à la jurisprudence Grenke Location). En outre, le CCAP pourrait être complété de stipulations prévoyant une faculté de résiliation unilatérale par les fournisseurs de services de cloud dans l'hypothèse où l'atteinte à la sécurité du cloud résulterait de la personne publique et où celle-ci ne serait pas en mesure d'y remédier. A l'instar de la suspension, la résiliation unilatérale ne serait envisageable qu'après que les fournisseurs aient mis les bénéficiaires à même de s'y opposer pour un motif d'intérêt général.

Liste des dispositions du CCAG-TIC inapplicables

Les dispositions visées ci-dessous ne seront pas applicables aux marchés publics de cloud, en ce qu'elles sont inadaptées à l'objet même du cloud. Il pourrait être envisagé, par souci de clarté, de lister dans le CCAP ces articles, en précisant qu'eu égard à leur caractère inadapté à l'objet même du cloud, ils ne seront pas applicables aux accords-cadres :

- les définitions de « logiciel », « logiciel standard », « logiciel spécifique » et « application » de l'article 2 - définitions, dès lors que les services cloud de type « SaaS » ne seront pas inclus dans l'objet du marché ;
- l'article 5.2 - Protection des données à caractère personnel, dès lors que les services cloud engendrent des traitements de données personnelles spécifiques qui doivent être encadrés de manière spécifique ;
- l'article 5.3 - mesures de sécurité, dès lors que les prestations objet du marché ne seront pas exécutées dans un lieu où des mesures de sécurité s'appliquent, telles que les zones protégées en vertu des dispositions législatives ou réglementaires prises pour la protection du secret de la défense nationale ;
- les articles 8.2, 8.3 et 11.6.2, dès lors que le marché ne sera pas un marché de fournitures ;
- l'article 13.2.2., dès lors que la réception des prestations ne se fera pas dans les locaux du prestataire ;
- l'article 13.2.3., dès lors que le marché n'a pas pour objet des prestations d'études ;
- les articles 14.2 - pénalités pour indisponibilité, 18 - aménagement des locaux destinés à l'installation du matériel objet du marché, 2 - mise à jour et nouvelles versions de logiciels, 24-4 - essais et bancs d'essais, 28.4.3., 29 - transfert de propriété, 30.6 - garantie de conformité des logiciels standards et 30.7 - logiciels libres, dès lors que le marché n'aura pas pour objet la fourniture de matériel ou de logiciels ;
- l'article 17 - moyens mis à disposition du titulaire, dès lors que le pouvoir adjudicateur ne devrait en principe mettre aucun moyen à la disposition du titulaire du marché ;
- les articles 19 - stockage, emballage et transport et 20 - livraison, dès lors que les prestations de service cloud n'impliquent ni stockage, ni emballage ni transport ;
- le deuxième alinéa de l'article 24.1 - point de départ du délai pour les opérations de vérification, dans la mesure où aucune vérification ne sera effectuée dans les locaux du pouvoir adjudicateur ;
- les articles 25 - vérifications quantitatives et 27.1, dans la mesure où ces vérifications sont adaptées à la fourniture de livrables mais pas à celle de services cloud ;
- les articles 28.2.3 et 28.4.3., 30.2, 30.4 et 30.5, dès lors que les notions d'enlèvement, d'évacuation, de destruction et de garde des prestations ajournées ou rejetées, de remplacement, frais de déplacement de personnel, emballage, transport de matériel, réparation et remises en état renvoient à la fourniture de livrables mais pas à celle de services cloud ;
- l'article 30 - garanties, dès lors que le marché ne portera ni sur la fourniture de matériels, ni sur celle de prestations dédiées ;
- le deuxième alinéa de l'article 31.2, dès lors que la notion de tierce maintenance applicative, qui renvoie aux « programmes informatiques », est sans relation avec les services de cloud ;
- les articles 32.2.1. et 32.2.2., dans la mesure où la maintenance ne sera pas effectuée dans les locaux du pouvoir adjudicateur ;
- l'article 42.1. b), dès lors qu'aucun moyen ne sera mis à la disposition du titulaire du marché par le pouvoir adjudicateur ou les bénéficiaires ;
- l'article 45 - remise des prestations et des moyens matériels permettant l'exécution des marchés, dans la mesure où aucune remise de quelque matériel ou prestation que ce soit ne sera envisageable au terme de l'exécution du marché.

À PROPOS

Cadre du rapport

Autour de CISPE (Cloud Infrastructure Services Providers in Europe), plusieurs associations professionnelles nationales de Cloud (Cloud Industry Forum, Danish Cloud Community, DHPA, EuroCloud France et EuroCloud Germany) se sont regroupées afin de promouvoir les politiques de Priorité Cloud (Cloud First) en Europe.

Dans le cadre de cette action, un guide d'achat destiné au acheteur du secteur public en Europe sera rendu public. Le présent document est la version française de ce document, adapté conjointement contexte français par les membres CISPE opérant en France et les membres d'EuroCloud France.

A propos de CISPE

CISPE (Cloud Infrastructure Services Providers in Europe) est l'association des fournisseurs d'infrastructure Cloud en Europe. Ses membres ont des sièges dans 15 pays Européens. CISPE est un partenaire de la co-régulaion et participe activement à la construction législative en Europe sur le Cloud.

CISPE a notamment développé le premier Code de conduite sectoriel permettant de démontrer la conformité de services d'Infrastructure Cloud avec le RGPD (Règlement Général sur la Protection des Données) : le « CISPE Data Protection Code of Conduct ». https://cispe.cloud/code-of-conduct/

A la demande de la Commission Européenne CISPE co-pilote avec EuroCIO (l'association des DSI européen) le premier Code de Conduite sur la portabilité des données non personnelles dans le IAAS demandé par le Règlement sur la Libre Circulation des données en Europe. https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security

A propos d'EuroCloud France

EuroCloud France est l'association professionnelle représentative du Cloud en France. Elle participe au débat public sur les sujets du numérique en France, et organise chaque année la Cloud Week Paris. Elle est composée de près de 150 membres.

EuroCloud FRANCE

CISPE.cloud

CISPE.cloud en partenariat avec EuroCloud FRANCE