

Le directeur général

Paris, le 18 juillet 2022  
N°255/ARM/DGNUM/SDTN/NP

**NOTE**

**à l'attention**

**des destinataires *in fine***

**OBJET** : politique d'hébergement des SI et des données sur INTERNET.

**RÉFÉRENCES** : a) note n°337/ARM/DGNUM/DG/DR du 22 septembre 2020 portant directive provisoire relative à l'accès à des services cloud en mode IaaS-PaaS hébergés à l'extérieur du ministère ;  
b) note N°458/ARM/DGNUM/DG/NP du 25 novembre 2019 portant directive provisoire relative à l'accès à des services cloud en mode SaaS hébergés à l'extérieur du ministère ;  
c) circulaire n°6282/SG du 5 juillet 2021 traitant de la doctrine d'utilisation de l'informatique en nuage par l'état.

**P. JOINTE** : « politique d'hébergement des SI et des données sur INTERNET ».

La DGNUM transmet en pièce jointe aux destinataires la « Politique d'hébergement des SI et des données sur INTERNET ».

Réalisée dans le cadre du chantier Hébergement Cloud, elle vise à définir le cadre d'hébergement des systèmes d'information et des données exposés sur INTERNET et en cela, constitue une aide aux directions d'application dans le choix de leur hébergement informatique en fonction des caractéristiques de leur projet.

Elle a été élaborée en prenant en compte le retour d'expérience des deux directives provisoires de référence a) et b), qu'elle abroge, et prend en compte les orientations fixées dans la doctrine Cloud de l'État de référence c).

Pour la mise en œuvre de cette politique, je vous demande de bien vouloir vous assurer de la mise en application de ce document au sein de vos états-majors, directions et services.

L'ingénieur général hors classe de l'armement Nicolas FOURNIER  
directeur général du numérique et des systèmes d'information  
et de communication  
**Original signé**

## LISTE DE DIFFUSION

### DESTINATAIRES :

- EMA/ESMG ;
- EMA/SNA ;
- DGA/S2NA ;
- SGA ;
- CGA ;
- DPID ;
- DRSD ;
- DICOD ;
- DC DIRISI ;
- DAJ ;
- AND.

### COPIES :

- EMA/COMCYBER ;
- EMAT ;
- EMM ;
- EMAAE ;
- DCSCA ;
- DCSSA ;
- DSEO ;
- DSIMu ;
- DRM ;
- DGA/DO ;
- SGA/DTPM ;
- DRH-MD ;
- DTIE ;
- DMCA ;
- DAF ;
- DGSE ;
- DGRIS ;
- Archives.

## **DOCUMENT DE POLITIQUE GENERALE**

# **Politique d'hébergement des SI et des données sur INTERNET**

Edition approuvée le 18/07/2022



**L'édition en vigueur de ce document est celle accessible via le site DGNUM.  
S'assurer de la validité de toute copie avant usage.**

		<b>Organisme</b>
<b>Rédaction</b>	IPETA Julien AUVRAY	DGNUM
<b>Vérification</b>	AEHC Olivier GANIS	DGNUM
<b>Approbation</b>	Tous membres du CECNUM	

## Table des matières

1. Contexte .....	6
1.1. Le besoin de SI sur INTERNET au sein du MinArm.....	6
1.2. Hébergement des SI et des données sur INTERNET .....	6
1.3. La doctrine Cloud de l'Etat.....	6
2. Orientations ministérielles pour l'hébergement des SI et des données sur INTERNET .....	6
2.1. Les différentes options d'hébergement pour le MinArm .....	6
2.2. Les critères de choix de l'hébergement .....	7
2.3. Points de vigilance concernant l'accès à Internet de l'utilisateur .....	9
3. Modalités d'accès aux services .....	10
3.1. C1 NP MinArm .....	10
3.2. C1 interministériel.....	10
3.3. C3 IaaS/CaaS/PaaS/SaaS du cloud public .....	10
3.3.1. Instruction du visa CLOUD DGNUM.....	10
3.3.2. L'avis du SC2A.....	10
3.3.3. Autres avis à associer à la demande de visa CLOUD.....	11
3.3.4. Rationalisation.....	11
3.4. Agrément du SIG.....	11
3.5. Homologation des SI .....	11
3.6. Pilotage, évaluation et révision de la politique .....	11
4. Textes abrogés.....	11
ANNEXE 1 - FEUILLE DE ROUTE DE L'OFFRE D'HEBERGEMENT INTERNE SUR INTERNET (C1-NP) .....	12
1. L'offre d'hébergement actuelle.....	12
2. L'offre d'hébergement cible .....	12
ANNEXE 2 - SYNTHÈSE DE LA DOCTRINE CLOUD DE L'ÉTAT DU 5 JUILLET 2021 .....	13
1. Le cloud, levier de la transformation numérique de l'Etat.....	13
2. Un recours généralisé aux technologies cloud.....	13
3. Une offre interne IaaS et SaaS existante et entretenue .....	13
4. Conditions d'accès aux clouds C3 .....	14
5. Un régime spécifique pour le MinArm .....	14
ANNEXE 3 - LE CLOUD COMPUTING : DEFINITION ET ENJEUX JURIDIQUES ET SECURITAIRES .....	15
1. Le cloud, ses services et ses typologies .....	15
1.1. Les différents services.....	15
1.2. Les différents types de cloud .....	16
2. Questions juridiques et confidentialité des données hébergées sur un cloud commercial.....	17
2.1. RGPD.....	17
2.2. L'exemple de la réglementation Américaine .....	17

2.3. Une insécurité juridique et économique qui doit être intégrée et maîtrisée dès la conception des projets de SI .....	18
ANNEXE 4 - QUESTIONNAIRE ET DONNEES A FOURNIR AVEC TOUTE DEMANDE DE VISA CLOUD DGNUM .....	19
1. Aspect Hébergement.....	19
2. Aspect Données .....	20
3. Aspect connexion .....	21
4. Aspect produits.....	21
5. Aspect gouvernance.....	22
ANNEXE 5 - portefeuille de SI hébergés sur INTERNET avec informations sur les services consommés .....	23

## 1. CONTEXTE

---

Le chantier ministériel « Hébergement cloud » chargé de définir la stratégie capacitaire de l'hébergement et des réseaux associés pour les prochaines années, a été lancé en avril 2021 par la Ministre des Armées (MinArm). Il comprend l'opération d'investissement « hébergement cloud », chargée de la fourniture et du maintien des différentes offres d'hébergement internes et mutualisées du ministère dont celles permettant l'exposition de services sur INTERNET, ainsi que le chantier « move to cloud » et la manœuvre RH nécessaire à sa réussite.

La présente politique d'hébergement des SI et des données sur Internet est réalisée dans le cadre de ce chantier ministériel. Elle vise à définir le cadre d'hébergement des SI et des données exposés sur INTERNET et en cela, constitue une aide aux directions d'application dans le choix de leur hébergement en fonction des caractéristiques de leur projet. Elle intègre également les orientations fixées dans la doctrine Cloud de l'État pour réguler l'accès aux offres de cloud commercial externes (dites « C3 ») par le MinArm.

### 1.1. Le besoin de SI sur INTERNET au sein du MinArm

Certains SI du MinArm sont déployés sur le réseau INTERNET à des fins opérationnelles, d'innovation, pour assurer des fonctions support (soutien, RH, formation, communication ...) ou pour fournir des services aux personnels du ministère des Armées n'ayant pas accès à un poste INTRADEF de manière permanente voire ponctuelle (exemple : crise sanitaire).

### 1.2. Hébergement des SI et des données sur INTERNET

L'hébergement des SI et des données sur INTERNET est réalisé soit sur des infrastructures informatiques internes (exemple : hébergement sur des infrastructures de la DIRISI ou du SSA exposées sur internet) soit sur des infrastructures informatiques externes (utilisation de services apportés par différents fournisseurs de services cloud comme OVH, Outscale, Scaleway, Orange, Bouygues et d'autres fournisseurs de services dont les hyperscaleurs américains Amazon Web Services, Google Cloud Platform, Microsoft Azure ...).

### 1.3. La doctrine Cloud de l'Etat

La doctrine Cloud de l'Etat du 5 juillet 2021 identifie le « Cloud computing » comme un des leviers essentiels de la transformation numérique de l'État et encourage les acteurs publics à s'emparer du cloud pour s'appuyer sur son potentiel afin de rendre un meilleur service, tout en gardant la maîtrise des données sensibles. Elle donne des critères pour le choix des offres de cloud commercial externes C3.

Une synthèse de la doctrine est proposée en annexe 2. L'annexe 3, propose quant à elle, une définition du cloud (et notamment des termes IaaS, CaaS, PaaS, SaaS, C1, C2, C3 utilisés dans la suite du document) et une description de ses enjeux juridiques et sécuritaires.

## 2. ORIENTATIONS MINISTERIELLES POUR L'HEBERGEMENT DES SI ET DES DONNEES SUR INTERNET

---

### 2.1. Les différentes options d'hébergement pour le MinArm

4 types d'hébergement sont possibles :

- **L'hébergement interne C1 NP MinArm** mentionné en Annexe 1 ;
- **L'hébergement externe C3 soumis exclusivement au droit français/européen**, qui se décompose en **deux types d'offre** :

- **l'offre publique commerciale qualifiée SecNumCloud<sup>1</sup>** : cette offre est pour le moment restreinte (OVH, Outscale et Worldline Cloud Services pour les offres IaaS) mais d'autres prestataires sont en cours de qualification par l'ANSSI. La liste en est tenue à jour sur le site de l'ANSSI ;
- **l'offre publique commerciale non SecNumCloud** : elle s'articule majoritairement autour des cloud français de type OVH, SCALEWAY, Outscale, Orange, SFR, Bouygues, ... et à la marge de cloud d'autres acteurs européens (T-Systems, Exoscale, ...) ;
- **L'hébergement externe C3 potentiellement soumis à une réglementation autre que le droit français/européen** : on retrouve avec cette offre tout type d'hébergeur, dont les hyperscaleurs Amazon Web Services, Google Cloud, et Azure.

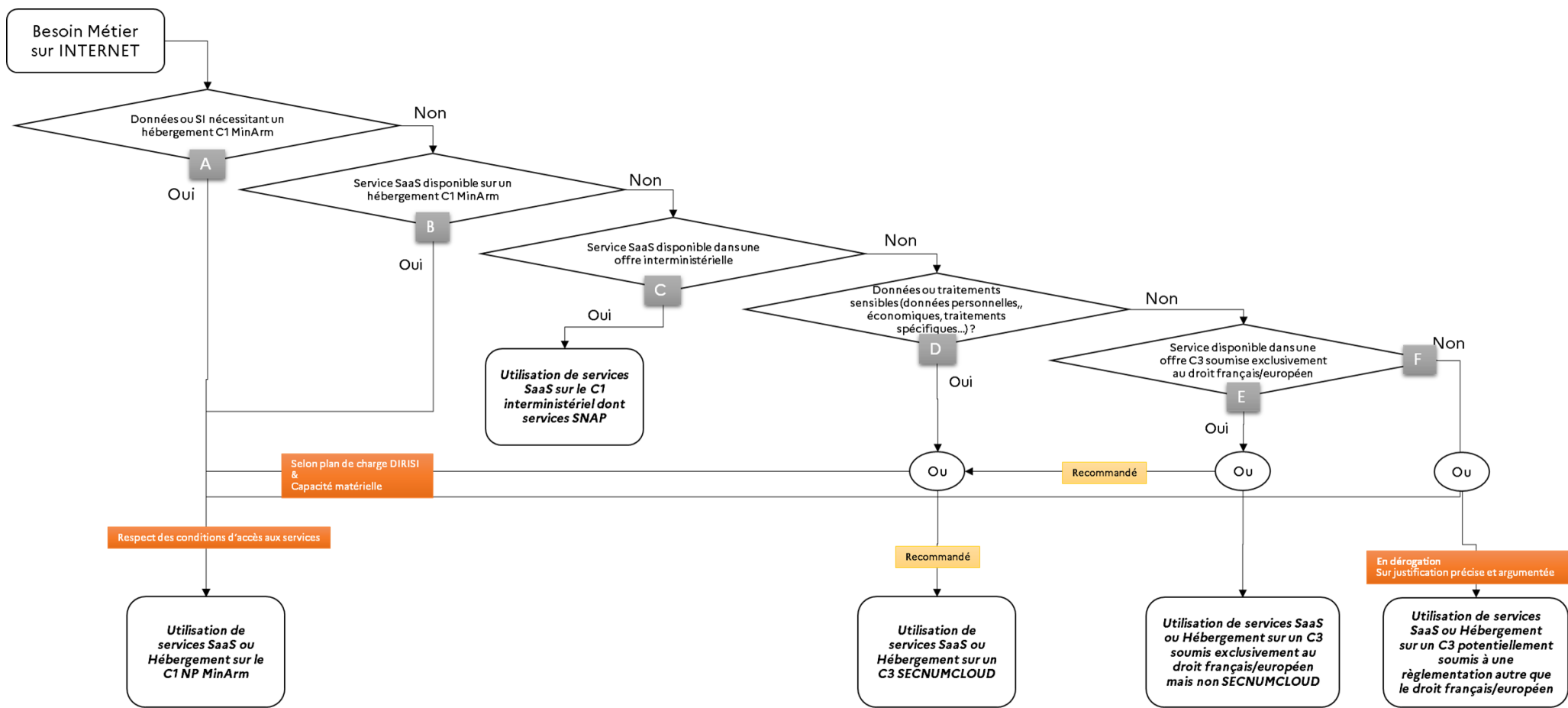
**Nota** : Il existe une offre de services SaaS développée et entretenue au niveau interministériel au travers du projet SNAP (Sac à dos Numérique de l'Agent Public) et d'autres projets (MENTOR par exemple) qui offrent un catalogue d'outils (webconférence, webinaire, plate-forme collaborative, ...) accessibles à tout agent public. L'accès à ces outils peut permettre de couvrir un certain nombre de besoins ministériels.

## 2.2. Les critères de choix de l'hébergement

Le logigramme ci-dessous présente les différentes possibilités d'hébergement en fonction des particularités du SI et de ses besoins en services.

---

<sup>1</sup> SecNumCloud définit un référentiel d'exigences, publié et maintenu par l'ANSSI, relatives au prestataire de service d'informatique en nuage (IaaS, CaaS, PaaS ou SaaS), à son personnel ainsi qu'au déroulement des prestations. La dernière version en vigueur est la version 3.2 du 8 mars 2022. Cette dernière version intègre notamment nativement des critères de protection vis-à-vis du droit extra-européen dans son paragraphe 19.6.



- A. Si le SI présente des enjeux de sécurité forts (exemple : site internet institutionnel du MinArm pour lequel une attaque cyber pourrait avoir des répercussions fortes en termes d'images, données sensibles précisées dans l'IM 900) et/ou des problématiques d'architectures complexes (exemple : interaction avec l'INTRADEF), alors l'hébergement doit être réalisé sur un C1 NP MinArm.
- B. Si la condition précédente n'est pas vérifiée et si le besoin peut être couvert par un service SaaS déjà disponible sur le C1 NP MinArm et ayant un niveau de qualité de service correspondant au besoin, alors celui-ci doit être utilisé ;
- C. Si les conditions précédentes ne sont pas vérifiées et si le besoin peut être couvert par un service SaaS déjà disponible sur le C1 NP Interministériel et ayant un niveau de qualité de service correspondant au besoin, alors celui-ci doit être utilisé ;
- D. Si les conditions précédentes ne sont pas vérifiées et si le SI manipule des données et traitements d'une sensibilité particulière (ce qui sera fréquemment le cas pour le MinArm car pouvant concerner à la fois les personnels du ministère et/ou traduire une activité opérationnelle), alors ce SI doit préférentiellement être hébergé sur un C3 NP certifié SecNumCloud. Le recours à un hébergement C1 ministériel est possible en fonction du plan de charge de la DIRISI et de la capacité disponible de cette solution d'hébergement.
- E. Si les conditions précédentes ne sont pas vérifiées et s'il existe une offre de services cloud C3 soumise exclusivement au droit français/européen<sup>2</sup> permettant d'offrir le service attendu, alors le SI doit être hébergé sur ce type d'hébergement, préférentiellement (si disponible) sur une offre qualifiée SECNUMCLOUD. Le recours à un hébergement C1 ministériel est possible en fonction du plan de charge de la DIRISI et de la capacité disponible de cette solution d'hébergement ;
- F. Enfin, **exceptionnellement**, sur justification précise et argumentée auprès de la **DGNUM**, si toutes les conditions précédentes ne sont pas réunies, un hébergement sur une offre C3 potentiellement soumise à une réglementation autre que le droit français/européen pourra être réalisé **par dérogation limitée dans le temps**. Si la dérogation n'est pas obtenue, alors le recours à un hébergement C1 ministériel sera à étudier en fonction du plan de charge de la DIRISI et de la capacité disponible de cette solution d'hébergement.

Il est également possible qu'un même projet consomme différentes solutions d'hébergement (notion d'hybridité de cloud) pour répondre à ses besoins. Par exemple, le projet SPARTA utilisera à la fois un hébergement C3 SecNumCloud (pour l'accès au service par les candidats au recrutement), un hébergement C1 NP MinArm (pour faire la passerelle INTERNET/INTRADEF) et un hébergement C1 Intradef (pour héberger les données les plus sensibles du processus de recrutement).

Pour tout hébergement sur le C1 NP, chaque SI devra se conformer aux conditions d'accès requises pour l'accès aux services offerts et fixées par la DIRISI (exemples : respect de la pile logicielle, automatisation via Ansible, authentification via MindefConnect ...).

### 2.3. Points de vigilance concernant l'accès à Internet de l'utilisateur

Il est de la responsabilité de la direction d'application, après accord de son autorité de domaine, de veiller à ce que l'usage de l'application hébergée sur INTERNET soit compatible avec les différents moyens d'accès à INTERNET et contraintes associées, fournis ou non par le ministère. Les différentes possibilités sont les suivantes :

- Postes INTERNET professionnel : ces postes maîtrisés par le MinArm sont raccordés directement à INTERNET (offre limitée) ;

---

<sup>2</sup> Le paragraphe 19.6 de la version 3.2 du 8 mars 2022 du référentiel SecNumCloud intègre des critères de protection vis-à-vis du droit extra-européen.

- Postes INTRADEF avec accès INTERNET via ISPT : ces postes maîtrisés par le MinArm déployés en grand nombre accèdent à internet via une passerelle filtrante (tous les types de flux ne sont pas autorisés) et limitée en nombre de licences (tous les postes n'en sont pas équipés) ;
- Postes et autres supports INTERNET personnel (BYOD) : l'usage de ces différents terminaux peut présenter des risques SSI et des difficultés réglementaires. L'usage reste de la responsabilité des autorités de domaines utilisateurs.

### 3. MODALITES D'ACCES AUX SERVICES

---

#### 3.1. C1 NP MinArm

L'accès aux offres C1 NP MinArm doit s'effectuer via l'outil DIADEME (<https://catalogue-services-dirisi.intradef.gouv.fr/sp>).

#### 3.2. C1 interministériel

Le catalogue de services SaaS C1 interministériel proposés ainsi que les modalités d'accès à ces services sont décrits sur les portails de services associés (par exemple pour le service MENTOR (formation) <https://www.fonction-publique.gouv.fr/la-formation-en-ligne> ou pour le Sac à dos Numérique de l'Agent Public <https://www.numerique.gouv.fr/outils-agents/>).

#### 3.3. C3 IaaS/CaaS/PaaS/SaaS du cloud public commercial

L'acquisition des services cloud C3 peut se faire en utilisant les marchés UGAP C3, Ouranos ou ceux ad-hoc (innovation, dédiés à un projet de SI, dédiés à des systèmes d'armes nécessitant le recours à des SI ...) à certaines entités du ministère. Toutes ces acquisitions sont concernées par une procédure de visa CLOUD de la DGNUM et soumises à l'ensemble des préconisations de gouvernance décrites ci-après. Cette procédure permet de garantir que le choix du fournisseur de services et les mécanismes de sécurité mis en place sont acceptables au regard des risques sur les données et les traitements prévus d'être effectués hors infrastructure MinArm. La procédure visa Cloud permet aussi de maintenir un inventaire de ces SI hébergés hors datacenters MinARM et ainsi faciliter la gestion de crise en cas d'incidents avec ces fournisseurs de service cloud.

##### 3.3.1. *Instruction du visa CLOUD DGNUM*

Tout accès à des services IaaS/CaaS/PaaS/SaaS sur le C3 doit faire l'objet d'un visa CLOUD de la DGNUM, instruit sur demande (NéMO) d'une direction d'application. Cette demande de visa devra obligatoirement contenir les données nécessaires à l'instruction de la demande (cf. questionnaire et données à fournir en annexe 4) ainsi que les avis évoqués aux § 3.3.2 et 3.3.3. Le visa est délivré par note de la DGNUM avec un période de validité et, le cas échéant, sous recommandations à respecter par le commanditaire.

Les différents responsables de pouvoirs adjudicateurs ministériels doivent s'assurer que le visa CLOUD a été obtenu avant de réaliser les commandes, quel que soit le marché sur lequel la commande est réalisée (marchés UGAP C3, marchés Ouranos, marchés spécifiques, marchés d'innovation, ...).

Il est recommandé de demander un avis préalable DGNUM à tout appel d'offres prévoyant le recours à des offres C3 afin de s'assurer que les clauses minimales sont prévues dans le cahier des charges. Un avis préalable DGNUM ne dispense pas de l'obligation d'obtention du visa CLOUD DGNUM postérieurement à l'appel d'offres.

##### 3.3.2. *L'avis du SC2A*

La saisine du sous comité de cohérence des architectures (SC2A) est obligatoire pour tout projet de SI, y compris ceux hébergés sur un cloud C3. En particulier, le SC2A pourra émettre des recommandations sur le choix de l'hébergement (C1 ou C3), l'architecture des SI (et en particulier, les éventuelles modalités d'interconnexion entre Internet et INTRADEF, les éléments de pile logicielle, ...). Une cohérence avec le cadre de cohérence technique (CCT) doit être recherchée pour toute refonte majeure de SI ou tout nouveau projet incluant un besoin IaaS, CaaS ou PaaS.

L'avis du SC2A est pris en compte dans l'instruction de la demande de visa CLOUD. Dans le cadre de demande de visa de courte durée pour des expérimentations ou des besoins ponctuels, le SC2A pourra décider de ne pas étudier le dossier.

### **3.3.3. Autres avis à associer à la demande de visa CLOUD**

La demande de visa CLOUD est impérativement associée à l'accord formel :

- du centre expert de l'AH concerné (bureau SSI de l'AH, OSSI central, OSSI des EMDS, etc.) ;
- du responsable de traitement dans le cadre d'un traitement de données à caractère personnel ; du DSI domaine (validation du besoin, cohérence du projet avec les autres projets du domaine, etc.).

### **3.3.4. Rationalisation**

Tout nouveau projet de SI (SaaS) doit réutiliser préférentiellement les outils SaaS déjà utilisés au sein du MinArm. La liste de ces services est entretenue par la DGNUM sur le site SYNOPTIC (<https://synoptic.intradef.gouv.fr/>).

### **3.4. Agrément du SIG**

Les SI hébergés sur INTERNET (en C1 ou en C3) dont l'objet est la communication institutionnelle, qui offrent des services à un large public (hors ressortissants du MinArm) ou qui sont des espaces dédiés dans des réseaux sociaux doivent faire l'objet d'un agrément du SIG selon les dispositions décrites dans la note N°458/DEF/DGSIC/DG/NP du 2 août 2016 ayant pour objet la mise en œuvre de services en ligne ou de sites Internet.

### **3.5. Homologation des SI**

La mise en service d'un service numérique utilisant des accès aux services IaaS/CaaS/PaaS/SaaS nécessite l'obtention d'une décision d'homologation par l'autorité d'homologation. La directive n°27 (<https://synoptic.intradef.gouv.fr/directive-ndeg27dgnum-3eme-edition-du-7-juin-2022-portant-sur-lhomologation-des-systemes>) en vigueur (DGNUM/DPID) portant sur l'homologation de sécurité du numérique en précise les modalités. La délivrance du visa CLOUD DGNUM ne dispense pas la direction d'application du respect de cette directive.

### **3.6. Pilotage, évaluation et révision de la politique**

Conformément aux dispositions précisées au §3.1.3 du guide relatif aux missions d'une DSI Domaine (1ère édition du 9 novembre 2021), les DSI Domaines portent la responsabilité de la maîtrise de leur parc applicatif. À cette fin, elles tiennent à jour un document exhaustif sur la situation de leur portefeuille de SI hébergés sur internet avec les informations sur les services consommés (cf. annexe 5). Ce document est présenté annuellement à la DGNUM pour lui permettre d'élaborer des tableaux de bord suivis en CECNUM. L'étude du contenu de ces portefeuilles permettra d'identifier les éventuels SI n'ayant pas fait l'objet de visa et de les remettre sous pilotage. Les DSI Domaines remettront également leurs éléments d'appréciation sur cette politique d'hébergement et les offres de services disponibles. Cette présentation en CECNUM sera l'occasion d'évaluer la présente politique et d'étudier d'éventuelles modifications à lui apporter au regard des évolutions de directives interministérielles, des offres de cloud externes et internes et des retours d'expériences apportés.

## **4. TEXTES ABROGES**

---

Les textes suivants sont abrogés par la présente politique :

- Note n°337/ARM/DGNUM/DG/DR du 22 septembre 2020 portant directive provisoire relative à l'accès à des services cloud en mode IaaS-PaaS hébergés à l'extérieur du ministère ;
- Note n°458/ARM/DGNUM/DG/NP du 25 novembre 2019 portant directive provisoire relative à l'accès à des services cloud en mode SaaS hébergés à l'extérieur du ministère.

## **ANNEXE 1 - FEUILLE DE ROUTE DE L'OFFRE D'HEBERGEMENT INTERNE SUR INTERNET (C1-NP)**

---

### **1. L'OFFRE D'HEBERGEMENT ACTUELLE**

---

A ce jour, l'hébergement des données et SI en interne MinArm est possible sur les 2 plates-formes suivantes :

- HELISS-NG (HEbergement d'appLications Internet sur SHéM Sécurisée Nouvelle Génération) : localisée au datacenter de Suresnes, elle a pour fonction l'hébergement sécurisé d'applications du ministère des Armées sur Internet. L'hébergement d'applications sur HELISS-NG nécessite le respect de la pile logicielle imposée par la plate-forme (hors dérogation SC2A). Le SI bénéficie d'une infogérance technique par la DIRISI hors composants déclarés comme non soutenus dans le CCT et qui ont fait l'objet d'une dérogation SC2A ;
- PHEBIA (Plate-forme d'hébergement Internet automatisée) : localisée au datacenter de Suresnes, elle permet d'héberger des SI NP dont les enjeux de sécurité ne sont pas très importants (à contrario d'HELISS-NG). L'exploitation de cette plate-forme est externalisée. Si le choix de la pile logicielle est plus libre que sur HELISS-NG, la totalité de l'infogérance de l'application ainsi qu'une partie des fonctions de sécurité, à savoir celles n'étant pas relatives à l'infrastructure d'hébergement, doivent être réalisées par la direction d'application.

Des éléments plus précis de description des services apportés par ces plate-forme sont disponibles sur le portail Hébergement de la DIRISI : <https://portail-hebergement.intradef.gouv.fr/index.php>.

### **2. L'OFFRE D'HEBERGEMENT CIBLE**

---

Un projet de remplacement d'HELISS-NG dit « C1-NP » est en cours avec une ouverture du service prévue pour 2023. Cette plate-forme C1 NP permettra d'héberger les SI nécessitant un haut niveau de sécurisation et avec un haut niveau d'automatisation s'appuyant sur les technologies cloud. Cette automatisation permettra d'une part d'accélérer les mises en production/exploitation des SI et, d'autre part, d'alléger la charge d'exploitation pour l'opérateur. Elle offrira également des environnements de développement et d'intégration, un accès à plusieurs services socles tels que la passerelle API pour les échanges avec Intradef, l'authentification MindefConnect, la gestion des secrets, ...

Dans un objectif de rationalisation des offres d'hébergement en une seule offre unique, l'hébergement PHEBIA, porté par la DIRISI, est prévu de s'arrêter fin 2024.

## **ANNEXE 2 - SYNTHÈSE DE LA DOCTRINE CLOUD DE L'ÉTAT DU 5 JUILLET 2021<sup>3</sup>**

### **1. LE CLOUD, LEVIER DE LA TRANSFORMATION NUMÉRIQUE DE L'ÉTAT**

---

La doctrine Cloud de l'Etat du 5 juillet 2021 identifie le Cloud computing comme un des leviers essentiels de la transformation numérique de l'État et encourage les acteurs publics à s'emparer du cloud pour s'appuyer sur son potentiel pour rendre un meilleur service, tout en gardant la maîtrise des données sensibles.

Elle répond aux enjeux suivants :

- Enjeu de transformation pour l'État en ce que le Cloud computing en est le facilitateur structurel. L'adoption du cloud doit s'accompagner de celle des pratiques associées à l'excellence dans la production de services numériques (proximité entre métiers et équipes informatiques, scalabilité, agilité, « devops », « continuous delivery » qui sont les garants de l'adaptation des produits à leurs utilisateurs) ;
- Enjeux de souveraineté et de sécurité : l'adoption du cloud ne doit pas entraver l'autonomie de prise de décision ni d'action de l'État, pas plus que sa sécurité numérique, la maîtrise par l'Etat des données et des traitements dont il est responsable, et ce alors que l'empreinte des acteurs extra-européens en matière de Cloud computing est prédominante ;
- Enjeu industriel : l'adoption du Cloud computing par l'État, et plus généralement par 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.

### **2. UN RECOURS GÉNÉRALISÉ AUX TECHNOLOGIES CLOUD**

---

La doctrine Cloud de l'Etat généralise le recours aux technologies cloud pour tout projet de SI. Elle s'applique aux services de l'État et aux organismes placés sous sa tutelle. Ainsi, tout nouveau projet et tout projet existant refondu à plus de 50%<sup>4</sup> devra utiliser ces technologies. Toute dérogation pour un projet supérieur à 1M€ sera à documenter. Pour vérifier l'application de ce principe, la DINUM prévoit d'une part d'intégrer le contrôle de ces dispositions pour tout projet soumis à l'article 3 du décret n° 2019-1088 du 25 octobre 2019. Aussi, au travers du pilotage du tableau de bord TOP50 des SI de l'Etat et du TOP250 des démarches simplifiées, des éléments d'informations concernant l'hébergement des SI sont à fournir par les ministères.

Le choix entre l'utilisation de cloud de type C1 ou de type C3 reste à discrétion des ministères. Ce choix pourra être fait sur la base de critères comme le niveau de sécurité, le coût complet de possession, les implications RH (en compétences et en nombre pour la direction d'application et l'opérateur), la nature des besoins techniques et fonctionnels et les choix d'urbanisation préalables.

### **3. UNE OFFRE INTERNE IAAS ET SAAS EXISTANTE ET ENTRETENUE**

---

La DINUM et les ministères associés entretiennent un catalogue d'offres de service Cloud. Ainsi, deux offres de services IaaS de type cloud C1 existent et sont disponibles pour l'ensemble des ministères :

- Le cloud PI géré par le Ministère de l'Intérieur ;
- Le cloud NUBO géré par la DGFIP.

---

<sup>3</sup> Circulaire n° 6282-SG du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'Etat

<sup>4</sup> Les modalités d'évaluation de ce seuil de 50% restent à définir.

La DINUM entretient également une offre de services SaaS nommée SNAP (Sac à doc Numérique de l'Agent Public) hébergés sur du C1 interministériel qui prend la forme d'un portefeuille de service à l'utilisateur. On y retrouve des services de messagerie instantanée (TCHAP), d'audioconférence, de web conférence, de portail de gestion de communauté (OSMOSE, RESANA), ...

*Nota : la DGNUM est l'interlocuteur ministériel privilégié pour relayer les demandes d'informations auprès des autres ministères et de la DINUM. Entre autres, de nombreux RETEX d'utilisation de services CLOUD des autres ministères sont disponibles sur la plate-forme OSMOSE.*

#### **4. CONDITIONS D'ACCES AUX CLOUDS C3**

---

La doctrine Cloud de l'Etat fixe un cadre quant à l'accès aux services cloud de type C3. Ainsi l'offre de cloud utilisée devra répondre aux exigences, potentiellement cumulatives, suivantes :

- Pour tout stockage / traitement de données personnelles, la conformité au RGPD<sup>5</sup> doit être assurée ;
- Pour tout stockage / traitement de données de santé, la conformité HDS doit être assurée ;
- Pour tout stockage / traitement de données d'une sensibilité particulière (données personnelles, données économiques, ... et hors données sensibles telles que définies dans l'IM 900), la conformité SecNumCloud<sup>6</sup> doit être assurée.

Plus généralement, pour tout projet de SI, la doctrine encourage le recours à des offres qualifiées SecNumCloud.

Pour les projets déjà lancés, la doctrine accorde un délai de mise en conformité de 12 mois, à compter de la disponibilité en France d'une offre de cloud « acceptable ». Ce caractère « acceptable » est défini dans la doctrine comme étant le point où les « éventuels inconvénients sont supportables ou compensables ».

Enfin, elle préconise de prévoir des mesures de réversibilité, portabilité, d'interopérabilité, de résilience et de sécurité pour tout SI hébergé sur un cloud de type C3.

#### **5. UN REGIME SPECIFIQUE POUR LE MINARM**

---

Le Ministère des Armées fait l'objet d'une dérogation dans l'application des modalités fixées par la doctrine (partie 1 du paragraphe 2.1 de la doctrine). Il est admis que pour l'optimisation de son socle ministériel devant traiter des SI autres que des SI de l'Etat (notamment les SI opérationnels qui ont des exigences spécifiques), le MinArm peut utiliser ses propres ressources et technologies d'hébergement. Cependant :

- les règles pour l'accès aux offres de cloud externes C3 sont applicables au MinArm ;
- la transformation vers des technologies cloud pour l'hébergement interne MinArm est un objectif ministériel.

---

<sup>5</sup> 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.

<sup>6</sup> SecNumCloud définit un référentiel d'exigences, publié et maintenu par l'ANSSI, relatives au prestataire de service d'informatique en nuage (IaaS, CaaS, PaaS ou SaaS), à son personnel ainsi qu'au déroulement des prestations. La dernière version en vigueur est la version 3.2 du 8 mars 2022. Cette dernière version intègre notamment nativement des critères de protection vis-à-vis du droit extra-européen.

## **ANNEXE 3 - LE CLOUD COMPUTING : DEFINITION ET ENJEUX JURIDIQUES ET SECURITAIRES**

---

La CNIL définit le cloud computing (en français, « informatique dans les nuages ») comme l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (cloud) composé de nombreux serveurs distants interconnectés.

### **1. LE CLOUD, SES SERVICES ET SES TYPOLOGIES**

---

#### **1.1. Les différents services**

Il existe 4 types de services apportés par le cloud IaaS, CaaS, PaaS et SaaS, tels que définis par l'ANSSI :

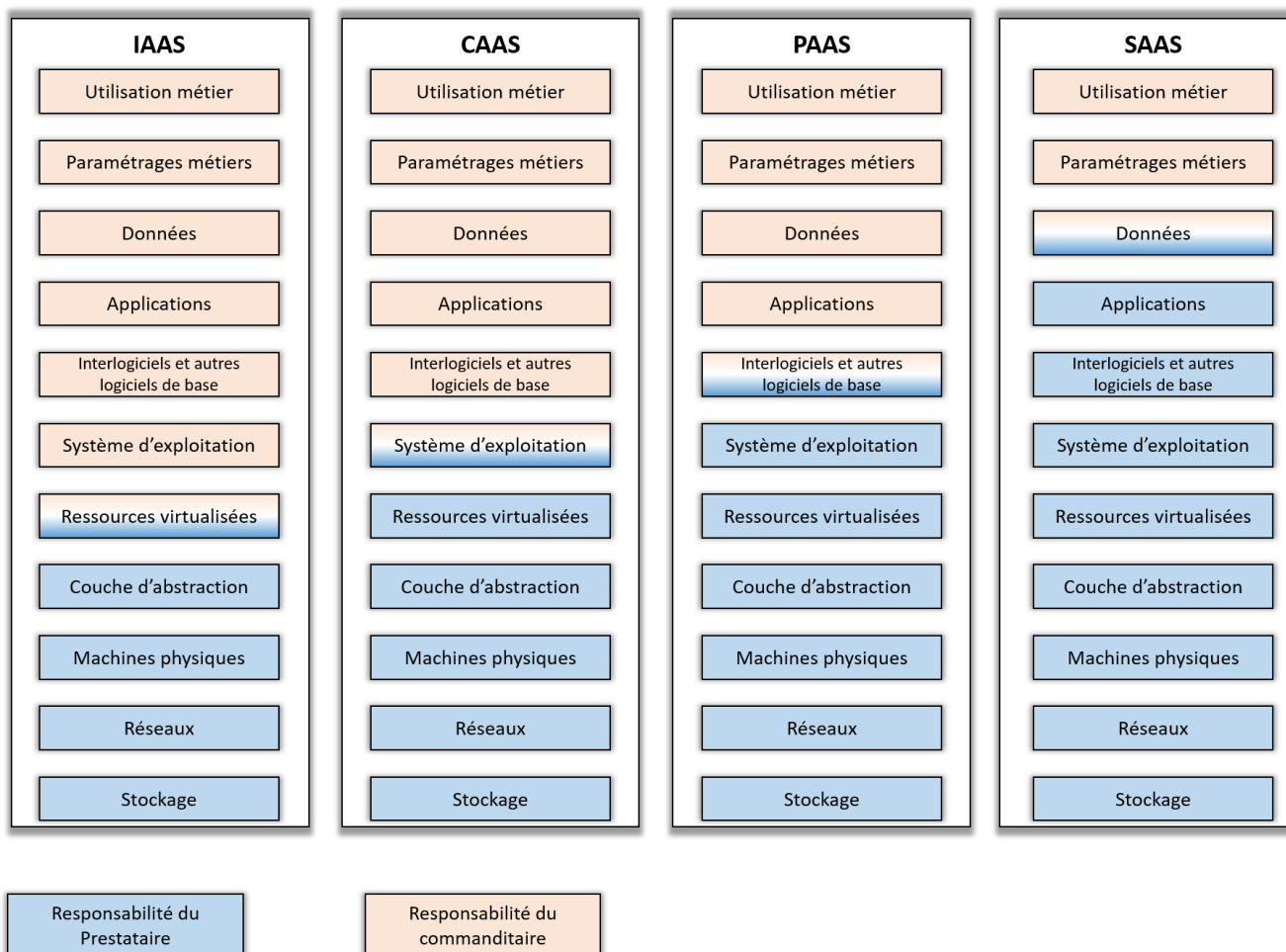
- L'Infrastructure as a Service (IaaS), ou infrastructure en tant que service, concerne la mise à disposition de ressources informatiques abstraites (puissance CPU, mémoire, stockage...). Le modèle IaaS permet au commanditaire de disposer de ressources externalisées, potentiellement virtualisées. Ce dernier garde le contrôle sur le système d'exploitation (OS), le stockage, les applications déployées ainsi que sur certains composants réseau (pare-feu...)
- Le Containers-as-a-Service (CaaS) concerne la mise à disposition d'environnements d'exécution permettant le déploiement et l'exécution de conteneurs. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente (réseau, stockage, serveurs, système d'exploitation), gérée et contrôlée par le prestataire. Le commanditaire a la maîtrise des outils systèmes, bibliothèques, intergiciels, et du code de l'application.
- Le Plateform as a Service (PaaS), ou plateforme en tant que service, est la mise à disposition par le prestataire de plateformes d'hébergement d'applications. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente, gérée et contrôlée par le prestataire (réseau, serveurs, OS, stockage...). Le commanditaire a cependant la maîtrise des applications déployées sur cette plateforme. Il peut ainsi avoir la maîtrise de certains services composant cette plateforme ou de certains éléments de configuration suivant la répartition des rôles définie dans le service.

Exemples : framework de type Apache, Tomcat, PHP et MySQL pour développer des applications web...

- Le Software as a Service (SaaS), ou logiciel en tant que service, la mise à disposition d'un logiciel sur une plateforme d'informatique en nuage. Le commanditaire n'a pas la maîtrise de la plateforme en nuage sous-jacente. Le prestataire gère de façon transparente pour le commanditaire l'ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d'effectuer quelques paramétrages métier dans l'application.

Exemples : « CRM », outils collaboratifs, messagerie, Business Intelligence, « ERP » ...

Le tableau ci-dessous présente le partage de responsabilité entre le prestataire et le commanditaire par type de service. Il est extrait du référentiel d'exigences des prestataires de services d'informatique en nuage (SecNumCloud) édité par l'ANSSI.



## 1.2. Les différents types de cloud

Les différents services cloud IaaS, CaaS, PaaS et/ou SaaS peuvent être mis à disposition au sein de différents types de Cloud. La stratégie cloud de l'Etat de 2018 identifiait les 3 types de cloud suivants :

- Le « cloud interne » dit C1 : les infrastructures et services sont hébergés en local. Ils adressent les applications et données sensibles.
- Le « cloud dédié » dit C2 : les infrastructures et services sont hébergés chez un opérateur et sont dédiés à l'organisation concernée. Ils adressent les applications et données de sensibilité moindres. Le cloud dédié C2 n'apparaît plus dans la doctrine « Cloud au centre » de 2021.
- Le « cloud externe » dit C3 : les infrastructures et services sont hébergées chez un opérateur et potentiellement mutualisées avec d'autres clients. Ils adressent les applications et données peu sensibles. Il est aussi appelé cloud commercial.

**Point d'attention :** Dans les offres type C3, la défendabilité et l'investigation post incident ne sont pas possibles en raison de l'impossibilité d'avoir accès à des journaux d'équipements mutualisés entre plusieurs clients (au mieux il est seulement possible d'avoir les journaux de niveau applicatif).

## 2. QUESTIONS JURIDIQUES ET CONFIDENTIALITE DES DONNEES HEBERGEES SUR UN CLOUD COMMERCIAL

### 2.1. RGPD

Sur le territoire de l'Union européenne, le RGPD s'applique. Son champ d'application dépend à la fois des modalités d'exercice de l'activité du fournisseur et de la personne dont les données personnelles sont traitées. S'il s'agit d'un citoyen européen ou résidant sur le territoire de l'Union européenne, donc une personne physique, le RGPD s'applique, quel que soit le lieu d'établissement du responsable de traitement ou celui de stockage des données.

Par ailleurs, le RGPD a prévu la situation où des données à caractère personnel de citoyens ou résidents européens peuvent être transférées vers des pays tiers ou à des organisations internationales, en les réglementant strictement.

### 2.2. L'exemple de la réglementation Américaine

Divers textes peuvent servir de base soit à l'interception des données en provenance de l'UE, soit à leur utilisation une fois en possession d'une entreprise régie par le droit américain (sous-traitante ou responsable de traitement). Le tableau ci-dessous propose une brève synthèse de ces lois et de leurs champs d'application.

TEXTES	DESCRIPTION	CHAMP D'APPLICATION
« <i>Foreign intelligence surveillance Act</i> » (FISA, 1978) Article 702 (2008)	Ce texte vise les fournisseurs de services de communications électroniques américains (y compris des services informatiques à distance). Le périmètre de la surveillance doit être certifié par le ministre de la justice et le directeur du renseignement national puis approuvé par le tribunal FISA en décrivant notamment le mode de communication ciblé (messenger, réseau social). Une fois approuvée, la surveillance est effectuée par les autorités publiques américaines qui fournissent à l'entreprise susceptible de détenir des informations des marqueurs (adresse mail, numéro de téléphone) qui s'appliqueront aux communications à destination ou en provenance de la personne.	<p><b>Champ d'application territorial</b> Le texte régit la surveillance <u>hors du territoire américain</u> des communications de <u>personnes non américaines</u> à des fins de renseignement.</p> <p><b>Champ d'application matériel</b> La cible est une <u>personne physique</u>. Ce dispositif ne vise pas exclusivement la lutte contre le terrorisme mais inclut la cybersécurité, la protection des forces armées américaines, le contre-terrorisme et la lutte contre la prolifération des armes.</p>
<i>Executive order</i> (EO) 12333 (1981)	Ce texte fonde le pouvoir, accordé par le Président des Etats-Unis, à une autorité publique (principalement la NSA) d'accomplir des enquêtes pour son compte. Il repose sur la collecte directe de données par l'autorité publique et par ses propres moyens techniques, par exemple en interceptant des communications vers les Etats-Unis (câbles sous-marins) qu'elles soient en transit ou à destination des Etats-Unis. Elle ne peut pas servir de fondement pour obliger une entreprise à fournir ces données.	<p><b>Champ d'application territorial</b> Le texte régit la surveillance <u>hors du territoire américain</u> des communications de <u>personnes non américaines</u> à des fins de renseignement.</p> <p><b>Champ d'application matériel</b> La cible peut être une <u>personne physique</u> ou une <u>personne morale</u>. Ce dispositif ne vise pas exclusivement la lutte contre le terrorisme mais inclut l'acquisition de renseignements étrangers importants, la lutte contre la prolifération d'armes de destruction massive et l'espionnage.</p>
« <i>Clarifying lawful overseas use of data</i> » (CLOUD) Act (2018)	Ce texte s'applique aux fournisseurs de services de communications américains. L'entité soumise au CLOUD Act est considérée comme l'entité donneuse d'ordre, capable de diriger les actions de ses filiales où qu'elles se trouvent. Le CLOUD Act peut donc servir de base à la collecte de données hors des Etats-Unis. Les demandes de communication de données, fondées sur le CLOUD Act, sont examinées par un juge américain qui vérifie l'existence d'un motif raisonnable de collecte.	<p><b>Champ d'application territorial</b> Le texte permet la communication de données <u>hors du territoire américain</u> (mais en « <i>possession, garde ou contrôle</i> » du fournisseur de services) de <u>personnes américaines et non américaines</u> à des fins de lutte contre la criminalité.</p> <p><b>Champ d'application matériel</b> La cible est une <u>personne physique</u>. Ce dispositif vise les enquêtes pénales portant sur un crime grave (acte de terrorisme, crime d'ordre économique par exemple) et commis sur le territoire américain.</p>

### **2.3. Une insécurité juridique et économique qui doit être intégrée et maîtrisée dès la conception des projets de SI**

La conciliation à opérer entre les lois de surveillance américaines d'une part et le RGPD d'autre part, reste une chose complexe pour les sociétés américaines, si bien qu'à ce jour il n'y a pas de consensus qui puisse se dégager. L'extra-territorialité américaine fait peser un risque important d'accès non maîtrisé aux données d'acteurs français dans le cadre de procédures administratives ou judiciaires introduites aux Etats-Unis. Cela représente à la fois un facteur d'insécurité juridique pour les acteurs publics, les entreprises et les citoyens et une menace en matière de sécurité économique, dans la mesure où les autorités américaines et des parties adverses sont susceptibles d'accéder à des informations, potentiellement sensibles, qui seraient divulguées dans le cadre d'une procédure d'enquête portant sur des « crimes graves », y compris en matière économique.

Ainsi, en synthèse, les paramètres à prendre en considération sont les suivants :

- nature des données : données à caractère personnel ou données non personnelles, données de personnes physiques (individus) ou de personnes morales (société, association, administration, collectivité etc.), données protégées par le secret de la défense nationale ;
- pays d'hébergement des données : territoire de l'Union européenne (UE) ou Etat tiers ;
- pays d'enregistrement des entités qui manipulent les données (société de droit européen ou de droit étranger y compris les prestataires).

Lorsque des données à caractère personnel de citoyens européens sont hébergées sur le territoire UE par une entité ou une chaîne d'entités régies par le droit européen alors le RGPD s'applique. Si ces données sont hébergées sur le territoire UE mais qu'une entreprise régie par le droit américain effectue des opérations pour le compte d'un donneur d'ordre européen, le RGPD reste applicable, en revanche il n'est pas exclu que les lois de surveillance américaines s'appliquent également.

Pour les données non personnelles (non DR et non classifiées), il n'existe pas de loi protectrice au niveau européen. La tendance est même plutôt à l'ouverture des données en Europe dans le sillage des initiatives type GAIA-X.

Les éléments de ce paragraphe ont été construits avec une analyse du référentiel juridique des Etats-Unis. Les mêmes questions peuvent se poser avec l'ensemble des pays ne faisant pas partie de l'Union européenne et notamment, la Chine (Cybersecurity law, Data security law, Personal information protection law), la Russie voire le Royaume-Uni.

# ANNEXE 4 - QUESTIONNAIRE ET DONNEES A FOURNIR AVEC TOUTE DEMANDE DE VISA CLOUD DGNUM

## 1. ASPECT HEBERGEMENT

Points d'étude	Oui/Non	Eléments de réponse
Disposez-vous d'un certificat d'hébergement de l'hébergeur du service et des données ? A fournir.		
L'hébergement prévu est-il certifié SecNumCloud (ANSSI) ?		
L'hébergeur de la solution/données est-il français ? Respecte-t-il les exigences du paragraphe 19.6 de la version 3.2 du référentiel SECNUMCLOUD de l'ANSSI ?		
La sauvegarde est-elle comprise dans le contrat d'hébergement ? Combien de temps les sauvegardes sont-elles conservées ? Comment les accès à ces sauvegardes sont-ils contrôlés ? Comment sont-elles détruites ?		
Le MCO/MCS est-il compris dans le contrat ?		
Quelle est la durée du contrat ?		
Existe-t-il un outil centralisé de journalisation des traces ?		
Où sont conservés les logs des traces ?		
Quels types de données figurent dans les logs ?		
Existe-t-il une méthodologie de récupération des logs ? (prévu au marché ?)		
Les flux sont-ils filtrés contre les diverses tentatives d'injection (SQL, XSS, XXE...) ?		
Existe-t-il une matrice des flux ?		
L'hébergeur détient-il une PSSI ? A fournir.		

## 2. ASPECT DONNÉES

Points d'étude	Oui/Non	Eléments de réponse
Avez-vous un dictionnaire ou une liste des données utilisées par le produit (types, domaine d'information, sensibilité des informations, ...) ? A fournir.		
Existe-t-il un PRA / PCA ? A fournir.		
L'hébergeur et/ou le titulaire fait-il appel à des sous-traitants ? Si oui, quels sont-ils, et dans quel cadre ?		
Quelles sont les données qui sont accessibles par les sous-traitants ?		
Les données sont-elles stockées en France, en Europe ou ailleurs ? Attestation à fournir.		
Y a-t-il des données personnelles traitées ?		
L'éditeur est-il certifié RGPD ? Certificat à fournir.		
En cas de DCP (Données à Caractère Personnel), une analyse d'impact a-t-elle été réalisée ? A fournir.		
Comment les données sont-elles transmises entre l'administration et le titulaire ?		
Le responsable de traitement de l'entité (DPO : Data Protection Officer) a-t-il donné un avis ? A fournir.		
Des trackers de webs analytics sont-ils mis en œuvre ?		
Y a-t-il un cloisonnement prévu pour les données MINARM (Machine Virtuelle ou Conteneur) ?		
Le prestataire autorise-t-il le chiffrement des données en amont sans posséder la clé de déchiffrement ?		
L'archivage (courant, intermédiaire et définitif) des données a-t-il été prévu ?		

### 3. ASPECT CONNEXION

Points d'étude	Oui/Non	Eléments de réponse
Quels sont le mode de connexion et les protocoles employés pour la protection des usagers et des administrateurs fonctionnels ?		
L'interopérabilité avec des mécanismes d'authentification de l'administration est-elle possible ?		
Quelle est la méthodologie de stockage des identifiants ?		
Quel est le modèle de gestion des accès et identités employé ? (IAM, IDaaS ou autre)		
Existe-t-il dans le produit des possibilités d'interconnexion avec d'autres services Internet ?		
Peut-on se connecter avec des profils de réseaux sociaux (Facebook, LinkedIn, YouTube et des viewers, Reader, spotify, daily motion ...) ?		
Des supers administrateurs au niveau prestataire sont-ils prévus et auront-ils des accès à des données (à préciser) ?		

### 4. ASPECT PRODUITS

Points d'étude	Oui/Non	Eléments de réponse
Est-ce un produit français ? européen ? non-européen ?		
Quel est le mode d'acquisition du produit ?		
Existe-t-il une politique de mise à jour et de corrections de vulnérabilité dudit produit ?		
Avez-vous une documentation du produit ?		

## 5. ASPECT GOUVERNANCE

Points d'étude	Oui/Non	Eléments de réponse
Est-ce une expérimentation ? Si oui quelle est sa durée estimative ?		
Quelle est la durée de vie de ce système en hébergement cloud ?		
Existe-t-il un produit similaire utilisé par la transformation numérique des armées ?		
Y a-t-il eu un passage en gouvernance du projet ?		
Existe-t-il une fiche SICLADE ?		
Un chef de projet et un RSSI ont-ils été nommés pour le suivi du projet ?		
Une démarche d'homologation a-t-elle été lancée ?		
Existe-t-il un cahier des charges ?		
Existe-t-il une clause de réversibilité pour les données (échéance de restitution des données, format de celles-ci, suppression totale des données chez l'hébergeur) ?		
Existe-t-il une politique de confidentialité du prestataire ?		
Existe-t-il une politique d'emploi pour pouvoir utiliser un service numérique public de type SaaS ?		
Existe-t-il un plan d'assurance sécurité émis par l'hébergeur, le prestataire ?		

## ANNEXE 5 - PORTEFEUILLE DE SI HEBERGES SUR INTERNET AVEC INFORMATIONS SUR LES SERVICES CONSOMMES

Projet					Service consommé						VISA				
Nom du projet	Description succincte du projet	THEME (SOCLE, SOUTIEN, RENS, ...)	Grand subordonné (EMA/DGA/SGA)	ENTITE	Type de service consommé (IaaS/PaaS/SaaS)	Marché (UGAP, OURANOS, Ad-HOC)	Nom du service	HEBERGEUR	Lieux hébergement	Certifications hébergement	Réf NÉMO	Réf visa	Délivrance	Durée (mois)	Fin validité
TN ARD	Visioconférence avec les personnels pour l'accompagnement de leur reconversion	SOCLE	SGA	ARD	SaaS	OURANOS	TIXEO	OVH	Roubaix	ISO 27002	NéMO N° ...	Note N° ...	01/01/2022	12	01/01/2023