Décret SREN : ce que les acteurs publics doivent savoir

Souveraineté numérique et conformité réglementaire pour les administrations publiques

Conformité cloud • souveraineté numérique • achats publics

Introduction

Publié au Journal officiel le 16 avril 2026, le décret d'application de l'article 31 de la loi SREN (Sécuriser et réguler l'espace numérique) marque un tournant pour la souveraineté numérique française. Il ne s'agit pas d'une formalité administrative supplémentaire, mais de la traduction juridique d'une prise de conscience : la dépendance technologique vis-à-vis de prestataires non souverains constitue un risque opérationnel réel, accentué par les tensions géopolitiques, l'instabilité des modèles économiques et les restrictions commerciales imprévisibles. Pour les organismes concernés, le compte à rebours est lancé : 18 mois pour se mettre en conformité. Cet article fait le point sur les trois questions essentielles à se poser.

1. Qui est touché ?

La première erreur serait de croire que tout le monde est concerné. Le décret vise un périmètre précis et explicitement défini : les administrations de l'État, les opérateurs de l'État et une liste nominative de six groupements d'intérêt public (GIP).

Ces six GIP sont :

- l'Agence du numérique en santé ;
- le Centre d'accès sécurisé aux données ;
- le Centre ressources prévention de la radicalisation ;
- le Collecteur analyseur de données ;
- la Modernisation des déclarations sociales ;
- le Système national d'enregistrement de la demande de logement social.

À l'inverse, une collectivité territoriale, un hôpital ou une structure parapublique qui ne figure pas dans ce périmètre n'est pas soumis aux mêmes obligations par défaut. La bonne première question n'est donc pas « que dois-je faire ? », mais « ce texte me concerne-t-il, et sur quels projets ? ».

Car même au sein des organismes visés, le décret ne s'applique pas à l'ensemble des traitements cloud. Il cible uniquement les données qui répondent à deux conditions cumulatives, c'est-à-dire qui doivent être réunies simultanément :

Condition 1 : une sensibilité particulière

La donnée relève d'un secret protégé par la loi (secret médical, secret des affaires, secret de la défense nationale, secret des procédures judiciaires) ou elle est nécessaire à l'accomplissement des missions essentielles de l'État : sécurité nationale, ordre public, protection de la santé. Le vade-mecum officiel cite des cas très concrets : les dossiers judiciaires du Parquet national antiterroriste, les données de régulation des interventions du SAMU, les messageries et outils collaboratifs des administrations, les systèmes de paye des agents publics exerçant des missions régaliennes, ou encore les résultats de recherche de l'INSERM et les brevets de l'INPI au titre du secret des affaires.

Condition 2 : un risque caractérisé

La violation de cette donnée doit être susceptible d'engendrer une atteinte concrète : à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes, ou à la protection de la propriété intellectuelle. Ce risque doit être suffisamment caractérisé, et non simplement hypothétique.

Un point capital, et souvent sous-estimé : dès lors qu'une seule donnée du système d'information déclenche les deux conditions, l'ensemble des données hébergées sur la même infrastructure doit être protégé au même niveau, sauf s'il existe un cloisonnement technique efficace, réalisable sans remettre en cause l'équilibre économique du contrat. Autrement dit, la qualification d'une donnée sensible peut « contaminer » tout un environnement d'hébergement.

2. Quels sont les enjeux ?

L'enjeu central du décret est de garantir que les données publiques les plus sensibles échappent à toute forme d'ingérence étrangère. Son article 2 mandate un référentiel élaboré par l'ANSSI, couvrant dix domaines d'exigence : organisation de la sécurité, gestion des ressources humaines impliquées dans le service, sécurité des systèmes d'information, cryptologie et contrôle d'accès, continuité d'activité, réversibilité, localisation de l'hébergement, contrôle capitalistique du prestataire, et, point d'orgue du dispositif, la protection contre tout accès par des autorités publiques d'un État tiers non autorisé par le droit de l'Union européenne.

Ce dernier critère est le cœur du sujet. Il vise directement les lois à portée extraterritoriale (de type Cloud Act) qui permettent à un État étranger d'exiger l'accès à des données hébergées par un prestataire relevant de sa juridiction, même si ces données sont physiquement stockées en Europe. C'est cette vulnérabilité que le décret entend neutraliser.

En pratique, ce référentiel reprend très largement les exigences de SecNumCloud, qui constitue à ce jour le seul niveau de conformité réellement opérationnel pour satisfaire à l'article 2. Le texte laisse la porte ouverte à une certification européenne d'un niveau au moins équivalent (en l'occurrence le schéma EUCS niveau High+), mais ce dernier n'existe pas encore sur le marché. Concrètement, les organismes concernés n'ont donc, pour l'instant, qu'une voie crédible.

Le deuxième enjeu est procédural et concerne les achats. Le décret introduit la notion d'« offre acceptable » : une offre est jugée acceptable si elle répond au besoin fonctionnel du projet, en tenant compte de son coût. Cette définition, en apparence anodine, change la donne dans les marchés publics. Elle oblige les acheteurs à documenter leur analyse de marché : quelles offres conformes existent, à quel prix, et pourquoi elles répondent (ou non) au besoin.

Trois conséquences en découlent pour les consultations à venir. D'abord, les critères de qualification cloud (conformité au référentiel, SecNumCloud) doivent apparaître explicitement dans les dossiers d'appel d'offres. Ensuite, les arbitrages économiques doivent être étayés par écrit, et non simplement invoqués. Enfin, la réversibilité, c'est-à-dire la capacité à récupérer et migrer ses données, devient un critère à part entière : un prestataire incapable de garantir la portabilité s'expose à une exclusion documentée.

L'enjeu de fond est donc double : technique (héberger au bon niveau de sécurité) et juridique (être capable de justifier, par écrit et de façon traçable, chaque choix cloud).

3. Comment répondre à cette obligation ?

Le délai de 18 mois peut sembler confortable ; il ne l'est pas, compte tenu de la complexité des migrations d'infrastructure et des contraintes de marchés publics. Voici la marche à suivre.

1. **Cartographier les projets cloud portant sur des données sensibles.** C'est le préalable indispensable. Il faut distinguer les projets en cours (qui peuvent bénéficier d'une dérogation et dont la migration doit être planifiée) des projets futurs (qui doivent être conçus conformes dès le départ). Cette cartographie permet d'identifier précisément le périmètre réellement soumis au décret, plutôt que de surréagir sur l'ensemble du SI.
2. **Anticiper la question de la dérogation.** Les organisations utilisant des offres non conformes sur des données sensibles disposent de 18 mois pour migrer, ou pour obtenir une dérogation renouvelable si aucune offre conforme n'est disponible. Attention : pour les projets engagés avant la publication du décret, cette dérogation n'est pas automatique. La demande est adressée à la DINUM via le ministre dont relève le projet ; la DINUM instruit le dossier sous deux mois, puis transmet un avis au Premier ministre. Les décisions sont publiées de façon motivée : vos justifications peuvent donc devenir publiques. Cela impose une rigueur particulière dans la construction du dossier.
3. **Réviser les critères d'appels d'offres,** en associant dès l'amont les fonctions achats, juridique et sécurité. La grille de décision commune n'est plus optionnelle : les critères de qualification cloud, les arbitrages économiques et la réversibilité doivent y figurer de manière structurée.
4. **Documenter les arbitrages dès maintenant.** C'est sans doute le conseil le plus important. Puisque les choix cloud devront pouvoir être expliqués, voire publiés, il vaut bien mieux formaliser les décisions au fil de l'eau qu'essayer de les reconstituer sous la pression d'un contrôle ou d'une demande de dérogation. Une traçabilité écrite des analyses de marché, des critères retenus et des raisons d'un choix constitue la meilleure protection.

Conclusion

Le décret SREN ne crée pas seulement une obligation technique d'hébergement souverain : il instaure une culture de la justification documentée des choix cloud pour les données sensibles de l'État. Les organismes concernés ont tout intérêt à ne pas attendre la fin du délai de 18 mois. Identifier son périmètre, planifier ses migrations, outiller ses appels d'offres et tracer ses décisions : ce sont les quatre chantiers à engager dès aujourd'hui pour aborder l'échéance sereinement, plutôt que dans l'urgence.

Article rédigé à visée informative, à partir de l'analyse du décret n° 2026-272 du 14 avril 2026 (article 31 de la loi SREN).

Le périmètre réel : qui est concerné ?

Trois bassins d'organismes visés, au-delà des six GIP souvent cités

Le décret est souvent présenté à travers la liste des six groupements d'intérêt public. C'est la partie la plus restreinte du dispositif. En réalité, trois catégories d'organismes sont visées, et le gros du volume se situe ailleurs.

LES TROIS BASSINS VISÉS PAR LE DÉCRET

Catégorie d'organismes	Volume	Source de référence
Administrations centrales et services déconcentrés de l'État	**~200**	Annuaire de l'administration, FSSI ministériels
Opérateurs de l'État (PLF 2026)	**431**	Jaune budgétaire opérateurs, data.gouv.fr
Groupements d'intérêt public nommément désignés	**6**	Article 1 du décret n° 2026-272

LES 6 GIP NOMMÉMENT DÉSIGNÉS

- Agence du numérique en santé
- Centre ressources prévention de la radicalisation
- Modernisation des déclarations sociales
- Centre d'accès sécurisé aux données
- Collecteur analyseur de données
- Système national d'enregistrement de la demande de logement social

POINT DE VIGILANCE : un dispositif encore incomplet

Le décret ne fixe que les grandes lignes du cadre. L'essentiel des exigences opérationnelles est renvoyé à un référentiel de l'ANSSI qui n'est pas encore publié. SecNumCloud reste à ce jour le seul niveau de conformité réellement opérationnel pour y répondre, mais le référentiel final pourra préciser ou compléter ces exigences. Le schéma européen EUCS niveau High, voie alternative prévue par le texte, n'existe pas encore sur le marché.

Êtes-vous concerné ? Le test en 4 questions

Auto-qualification en moins de 2 minutes, à faire projet par projet

Q1 Mon organisation est-elle visée ?

OUI Administration de l'État, l'un des 431 opérateurs, ou l'un des 6 GIP listés.

→ Passez à Q2

NON Collectivité, hôpital, association, structure parapublique non listée.

→ Non concerné par le décret

Q2 Mon projet traite-t-il des données à sensibilité particulière ?

OUI Secret protégé par la loi (médical, défense, judiciaire, affaires) OU donnée nécessaire aux missions essentielles de l'État.

→ Passez à Q3

NON Données de gestion courante, communication banale, sans secret ni enjeu régalien.

→ Non soumis pour ce projet

Q3 La violation créerait-elle un risque caractérisé ?

OUI Atteinte concrète et caractérisée à l'ordre public, la sécurité, la santé, la vie des personnes ou la propriété intellectuelle.

→ Passez à Q4

NON Risque seulement hypothétique ou théorique, sans impact concret identifiable.

→ Non soumis pour ce traitement

Q4 Une donnée sensible partage-t-elle l'infrastructure ?

OUI Une seule donnée qualifiée contamine tout l'hébergement, sauf cloisonnement technique efficace et prouvé.

→ OBLIGATION : hébergement SecNumCloud

NON Infrastructure strictement cloisonnée, aucune donnée sensible n'y transite.

→ Non soumis pour cet hébergement

OBLIGATION CONFIRMÉE

Hébergement qualifié SecNumCloud requis. 18 mois pour migrer (échéance 17 octobre 2027) ou demande de dérogation. Voir le kit page 10.

NON CONCERNÉ (à ce stade)

Documentez l'analyse par écrit. Réévaluez à chaque nouveau projet et à chaque évolution. Les bonnes pratiques cloud souverain restent recommandées.

Réflexe utile

Le test se fait projet par projet, pas organisation par organisation. Un même organisme peut avoir des projets soumis et d'autres non. En cas de doute sur Q2 ou Q3, tranchez avec le RSSI et le juriste : la qualification engage la responsabilité de l'acheteur.

Quels sont les risques ?

Ce que la non-conformité expose, côté organisme public et côté prestataire

Le décret ne prévoit pas d'amende administrative de type RGPD pour l'organisme public. Les risques sont ailleurs : ils touchent la recevabilité des marchés, la responsabilité de l'acheteur, la réputation et, surtout, l'exposition à une ingérence étrangère.

POUR L'ORGANISME PUBLIC (acheteur)

Recevabilité de l'offre
Une offre non qualifiée peut être éliminée immédiatement (inversion des phases d'analyse). Conséquence : AO relancé, projet retardé.

Responsabilité documentée
L'acheteur doit justifier ses arbitrages par écrit. Un défaut de traçabilité l'expose en cas de contrôle ou de recours.

Dérogation rendue publique
Les décisions de dérogation sont motivées et publiées sur data.gouv.fr. Risque réputationnel direct.

Exposition à l'ingérence étrangère
Cœur du dispositif : un hébergement non souverain expose les données aux lois extraterritoriales (type Cloud Act) et à un accès par une autorité étrangère.

POUR LE PRESTATAIRE CLOUD (à connaître pour qualifier vos engagements)

Pénalité de 20 % du marché
Pénalité forfaitaire en cas de manquement à la clause de réversibilité (clause-type DAJ).

Résiliation sans mise en demeure
La perte de qualification entraîne une résiliation de plein droit du marché.

Exclusion documentée
Un prestataire incapable de garantir la portabilité des données peut être exclu, de façon tracée.

Cascade sous-traitants
Les sous-traitants et fournisseurs doivent eux-mêmes justifier d'une qualification équivalente.

À retenir

Le risque dominant n'est pas financier au sens d'une sanction, mais opérationnel et stratégique : un marché irrecevable ou résilié, un projet bloqué faute d'offre conforme, une dérogation publiée, et la perte de maîtrise sur des données sensibles face à une puissance étrangère. Anticiper coûte beaucoup moins que subir l'un de ces scénarios à l'approche d'octobre 2027.

Quick list et qualification des données

Les 4 chantiers immédiats et un tableau de référence par type de traitement

QUICK LIST : 4 chantiers à engager avant octobre 2027

1 Cartographier

Recenser tous les projets cloud traitant des données potentiellement sensibles. Séparer projets en cours (dérogation possible) et projets futurs (conformité dès la conception).

2 Qualifier

Appliquer les 2 conditions cumulatives à chaque projet. Attention à l'effet de contamination : une donnée sensible impose SecNumCloud à toute l'infrastructure. Associer DSI, RSSI, juriste et métier.

3 Outiller les achats

Intégrer les 6 clauses CCAP (qualification à l'offre, audit, destruction, pénalités, résiliation, réversibilité) dans les AO. Source : fiche DAJ du 6 mai 2026.

4 Tracer

Documenter chaque décision cloud dès maintenant. Les justifications de dérogation sont publiées sur data.gouv.fr. Une traçabilité continue vaut mieux qu'une reconstitution sous pression.

TABLEAU DE QUALIFICATION : exemples concrets

Type de traitement / donnée	Sensibilité ?	Risque caractérisé ?	Décret ?
Messageries et outils collaboratifs des agents de l'État	**OUI**	**OUI**	**OUI**
Dossiers judiciaires (Parquet national antiterroriste)	**OUI**	**OUI**	**OUI**
Données SAMU et régulation médicale d'urgence	**OUI**	**OUI**	**OUI**
Systèmes de paye des agents exerçant des missions régaliennes	**OUI**	**OUI**	**OUI**
Brevets INPI et résultats de recherche INSERM (secret affaires)	**OUI**	**OUI**	**OUI**
Logiciel RH classique sans donnée régalienne	**NON**	**NON**	**NON**
Site web institutionnel sans donnée sensible	**NON**	**NON**	**NON**
Données d'une collectivité locale (hors périmètre opérateurs)	–	–	**Hors champ**

Tableau indicatif. La qualification finale relève de l'organisation concernée, avec son RSSI et ses conseils juridiques. Sources : décret n° 2026-272 · vade-mecum ANSSI · fiche DAJ du 6 mai 2026.

Kit de mise en conformité : comment gérer

Le playbook opérationnel, étape par étape, et qui fait quoi

LE PLAYBOOK EN 5 PHASES

Phase 0 **Gouvernance** *Avant tout*	Désigner un référent SREN et constituer une cellule projet réunissant DSI, RSSI, achats, juridique et représentants métier. Sans pilotage transverse, la conformité échoue.
Phase 1 **Cartographier** *Mois 1 à 2*	Inventorier les projets cloud et les flux de données. Pour chacun, appliquer le test des 2 conditions. Produire un tableau de bord par projet avec son statut de qualification.
Phase 2 **Décider** *Mois 2 à 4*	Pour chaque projet soumis : conforme (rien à faire), à migrer (planifier), ou dérogation (monter le dossier). Arbitrer selon la disponibilité d'une offre acceptable sur le marché.
Phase 3 **Outiller les achats** *Mois 3 à 6*	Réviser les modèles d'appel d'offres et de CCAP. Intégrer la qualification exigée à l'offre, les 6 clauses obligatoires et le critère de réversibilité. Documenter l'analyse de marché.
Phase 4 **Migrer ou déroger** *Mois 6 à 18*	Exécuter les migrations vers une offre qualifiée, ou déposer les demandes de dérogation auprès de la DINUM via le ministère de tutelle. Suivre l'avancement jusqu'à l'échéance d'octobre 2027.

QUI FAIT QUOI : la répartition des rôles

DSI	Pilote la cartographie et les migrations techniques	**RSSI**	Qualifie la sensibilité des données, valide le niveau de sécurité
Juridique / DAJ	Sécurise les clauses contractuelles et les dossiers de dérogation	**Acheteur**	Révise les AO, documente l'analyse de marché et les arbitrages
Métier	Identifie les données réellement manipulées et les usages	**Direction**	Arbitre, porte le calendrier et engage la responsabilité de l'organisme

Contacts et ressources utiles

Dérogation : demande adressée à la DINUM via le ministre de tutelle (instruction 2 mois, avis au Premier ministre, décision publiée sur data.gouv.fr). Référentiel et qualification : ANSSI (cyber.gouv.fr). Clauses-types et fiche technique : DAJ de Bercy (economie.gouv.fr/daj). Liste des opérateurs : jaune budgétaire PLF 2026 (data.gouv.fr).

Dérogation, clauses et calendrier

Ce qu'il faut intégrer dans vos marchés et votre planning de conformité

MÉCANISME DE DÉROGATION (arrêté du 14 avril 2026)

Conditions cumulatives :
1. Projet cloud engagé AVANT le 17 avril 2026
2. Aucune offre conforme acceptable disponible sur le marché

Procédure : organisme → ministère de tutelle → DINUM (2 mois) → Premier ministre → décision publiée (data.gouv.fr)

18 mois	1 an renouvelable
Si une offre acceptable existe en France	Si aucune offre acceptable disponible

6 CLAUSES CCAP OBLIGATOIRES (fiche DAJ du 6 mai 2026)

Art. 1 : Qualification à l'offre
Qualification SecNumCloud ou équivalent prouvée dès la remise de l'offre, sous peine de rejet.

Art. 2 : Maintien de la qualification
Maintien pendant toute la durée du contrat, avec notification immédiate de toute perte.

Art. 3 : Droit d'audit
Audit possible avec préavis de 2 mois minimum, portant sur la sécurité et la conformité.

Art. 4 : Destruction documentée
Destruction des données en fin de contrat, avec procès-verbal contresigné.

Art. 5 : Pénalités spécifiques
Pénalités dédiées en cas de manquement, distinctes des pénalités de retard classiques.

Art. 6 : Résiliation de plein droit
La perte de qualification entraîne résiliation sans mise en demeure préalable.

CALENDRIER : échéance 17 octobre 2027

Décret en vigueur	Cartographie	Révision des AO	ANSSI à venir	Migrations	Échéance
17/04/2026	Mois 1-2	Mois 3-6	Référentiel	Mois 6-18	17/10/2027

TransfertPro, solution opérationnelle dès aujourd'hui :

Hébergement sur infrastructure 3DS Outscale qualifiée SecNumCloud · CSPN ANSSI SaaS et OnPremise · conforme aux exigences du décret.

Idées reçues et questions fréquentes

Les objections les plus courantes, et ce que dit réellement le décret

"Nous sommes certifiés ISO 27001 ou HDS, cela suffit."

→ Non. Ces référentiels portent sur la sécurité ou les données de santé, mais ne répondent pas au risque d'accès par une autorité étrangère. Seule une qualification SecNumCloud (ou une certification européenne de niveau au moins équivalent) satisfait l'article 2 du décret.

"Le schéma européen EUCS va arriver, autant attendre."

→ Le niveau EUCS High prévu par le texte n'existe pas encore sur le marché. À ce jour, SecNumCloud est la seule voie crédible. Attendre, c'est risquer de rater l'échéance du 17 octobre 2027 compte tenu de la durée des migrations.

"Nous sommes en cloud privé ou en interne, donc hors champ."

→ Le décret vise les services cloud fournis par un prestataire privé. Un hébergement strictement interne peut être hors champ, mais dès qu'un prestataire privé intervient sur des données sensibles, la qualification s'impose.

"Petit opérateur, peu de données : nous ne sommes pas concernés."

→ La taille n'entre pas en compte. Ce qui qualifie un projet, c'est la nature des données (les 2 conditions cumulatives) et l'effet de contamination : une seule donnée sensible suffit à imposer le niveau requis à toute l'infrastructure.

"Le référentiel ANSSI n'est pas publié, on attend."

→ Le cadre et l'échéance sont déjà fixés, et SecNumCloud est déjà la référence opérationnelle. Attendre le référentiel final ne fait que réduire le temps disponible pour cartographier, arbitrer et migrer.

"SecNumCloud, c'est trop cher et trop lourd pour nos usages."

→ Des offres SaaS qualifiées existent déjà, pas seulement des infrastructures brutes. Le coût se compare au risque évité : rejet d'appel d'offres, dérogation publique, exposition à une ingérence étrangère.

Référence officielle : Télécharger le décret n° 2026-272 du 14 avril 2026 sur Légifrance (Journal officiel de la République française).

À propos de TransfertPro

TransfertPro est une solution souveraine de transfert et de partage sécurisé de fichiers sensibles, destinée aux administrations publiques, aux entreprises stratégiques et aux organismes soumis à des exigences de conformité élevées. Les données sont traitées dans un cadre français et européen, sans accès de TransfertPro au contenu des fichiers (chiffrement AES-256, clés inaccessibles).

NOS CERTIFICATIONS PRODUIT (TransfertPro)

- ✓ Certification ANSSI CSPN, version SaaS (Réf. ANSSI-CSPN-2025/14)
- ✓ Certification ANSSI CSPN, version OnPremise
- ✓ Qualification élémentaire ANSSI et Visa de sécurité 2025

NOTRE INFRASTRUCTURE D'HÉBERGEMENT (3DS Outscale)

- ✓ Hébergement qualifié SecNumCloud (3DS Outscale)
- ✓ Certifié HDS, hébergement de données de santé
- ✓ Certifié TISAX, sécurité de l'information

Distinction importante pour les acheteurs publics

SecNumCloud, HDS et TISAX sont les qualifications de notre hébergeur 3DS Outscale. TransfertPro s'appuie sur cette infrastructure qualifiée. Les certifications CSPN, elles, portent directement sur le produit TransfertPro. Cette distinction est conforme à la logique de traçabilité du décret SREN.

COORDONNÉES

TransfertPro
32 Boulevard de Courcelles, 75017 Paris
contact@transfertpro.com
https://www.transfertpro.com
+33 (0)1 42 27 30 20

Document à visée informative, établi à partir de l'analyse du décret n° 2026-272 du 14 avril 2026 (article 31 de la loi SREN).