FICHE PRATIQUE

MAJ · Mai 2026

Article 31 - Loi SREN

Protection des données sensibles dans le cloud privé · Décret d'application du 14 avril 2026

Contexte

L'article 31 de la loi SREN (21 mai 2024) impose aux acheteurs publics de recourir exclusivement à des services cloud qualifiés **SecNumCloud 3.2** dès lors qu'ils traitent des données d'une sensibilité particulière. Le décret du 14 avril 2026 fixe les modalités d'application et les dérogations.

1 - CHAMP D'APPLICATION

Qui est concerné ?

- **Administrations de l'État :** Ministères, services centraux et déconcentrés
- **Opérateurs de l'État :** 431 opérateurs listés en annexe du PLF 2026 (data.gouv.fr)
- **GIP désignés par décret :** Agence du numérique en santé (ANS), CASD, Health Data Hub, GIP MDS, GIP SNE, Centre ressources radicalization…

Quel service cloud ?

Tout service d'informatique en nuage (IaaS, PaaS, SaaS) **fourni par un prestataire privé** dès lors qu'il traite des données sensibles au sens de l'art. 31.

Périmètre précis : Uniquement le cloud privé commercial. Les solutions internes (cloud interministériel) ne sont pas soumises à cet article.

Double condition CUMULATIVE

Condition 1 - Sensibilité des données
Les données relèvent de secrets protégés par la loi (art. L.311-5 et L.311-6 CRPA) ou sont nécessaires à l'accomplissement des missions essentielles de l'État : sauvegarde de la sécurité nationale, maintien de l'ordre public, protection de la santé et de la vie des personnes.

Condition 2 - Risque caractérisé d'atteinte
La violation de ces données doit être susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé ou à la vie des personnes, ou à la propriété intellectuelle. Ce risque doit être suffisamment caractérisé — non simplement hypothétique — et constituer la conséquence directe de la violation.

Exemples de données concernées :

- Applications d'aide au traitement des **dossiers judiciaires criminels**
- Systèmes d'information des **chaînes d'alerte sanitaire et de secours**
- Données relatives à la **paye des agents publics**

2 - MISE EN OEUVRE - RÉFÉRENTIEL SECNUMCLOUD 3.2

Qualification SecNumCloud 3.2

Le prestataire doit être qualifié par l'ANSSI dans sa version 3.2, ou détenir une certification d'un État membre de l'UE/EEE offrant un niveau de protection équivalent. La qualification est attestée dans le cadre du chapitre III du décret n°2015-350.

Organisation sécurité & exploitation

Le référentiel ANSSI fixe les **exigences en matière d'organisation de la sécurité de l'information**, de gouvernance, de gestion des risques, de continuité d'activité et des modalités d'exploitation du service cloud.

Clauses contractuelles obligatoires

Le contrat doit intégrer des clauses portant sur : maintien de la qualification, gestion des sous-traitants, transmission des audits, destruction certifiée des données, réversibilité et portabilité, droits d'audit de l'acheteur.

Localisation & transferts hors UE

Les **données sensibles doivent être hébergées dans l'UE**/EEE. Tout transfert vers un État tiers doit être encadré et conforme au droit de l'UE. Les accès par des autorités publiques d'États tiers non autorisés par le droit européen sont explicitement proscrits.

OPTION D'ACHAT SIMPLIFIÉ
Le catalogue UGAP propose des offres qualifiées SecNumCloud 3.2. L'administration peut aussi organiser elle-même une procédure d'attribution - dans ce cas, les clauses-types DAJ (règlement de consultation + CCAP) doivent être utilisées.

Source : Décret n°2026-272 du 14 avril 2026

3 - BONNES PRATIQUES À L'USAGE DES ACHETEURS

1 Cartographier les données

Réaliser une analyse au cas par cas pour **identifier les systèmes d'information traitant des données d'une sensibilité particulière au sens de l'art. 31**. S'appuyer sur le Vade-mecum DINUM disponible sur *numerique.gouv.fr*. La cartographie doit distinguer données à caractère personnel renforcé et données sensibles au sens SREN.

2 Choisir le bon mode d'hébergement

Privilégier le cloud interministériel interne pour les données très sensibles. Pour les offres commerciales, consulter la circulaire n°6519/SG (5 fév. 2026) sur la commande publique numérique et la circulaire n°6282/SG (5 juil. 2021) sur la doctrine cloud de l'État. **Vérifier que l'offre retenue dispose de la qualification SecNumCloud 3.2**.

3 Contractualiser avec les clauses-types DAJ

Règlement de consultation : intégrer la clause I.A (qualification comme critère éliminatoire dès l'offre). CCAP (clauses I.B) : qualification, audits de sécurité (art. 2), destruction des données + PV contradictoire (art. 3), documentation et droits d'accès (art. 4), pénalités en cas de non-respect (art. 5), résiliation pour perte de qualification sans mise en demeure (art. 6).

4 Assurer la réversibilité & souveraineté

Intégrer les clauses II de l'annexe DAJ : propriété du code source (§1.2), propriété intellectuelle des résultats (art. 2). Prévoir la documentation technique en français, les interfaces en français et un support de premier niveau francophone. Appliquer l'art. 46.2.3 du CCAG TIC : les données générées appartiennent exclusivement à l'acheteur. **Désigner le tribunal administratif compétent et le droit français applicable**.

A savoir

Les organisations utilisant des offres non conformes sur des données sensibles disposent de 18 mois pour migrer - ou bénéficient d'une dérogation renouvelable si aucune offre conforme n'est disponible. Pour les projets engagés avant la publication du décret, cette dérogation peut être demandée à la DINUM via le ministre dont relève le projet. Elle instruit le dossier dans un délai de deux mois, puis émet un avis transmis au Premier ministre. Les décisions sont publiées de façon motivée : les justifications peuvent devenir publiques.

Dates clés

21 mai 2024	5 fév. 2026	14 avr. 2026	16 avr. 2026	17 avr. 2026
Publication de la loi SREN	Circulaire sur la commande publique numérique	Décret d'application + arrêté dérogation	Date de référence dérogations	Le décret entre en vigueur