cloud-store.fr

Solutions logicielles pour le secteur public

■ LIVRE BLANC | 2025

Télémaintenance & RGPD : Comment choisir une solution conforme pour les organismes publics et entreprises sensibles

Modèles de déploiement • Certifications éditeurs
Points de vigilance ANSSI • Comparatif solutions

■ cloud-store.fr | ■ contact@cloud-store.fr | ✎ Contactez-nous : cloud-store.fr/contact/

Sommaire

■ Ce livre blanc est destiné aux DSI, RSSI et responsables achats des collectivités territoriales, établissements publics, ministères et entreprises soumises à des obligations de sécurité renforcées. Il a pour but de vous aider à choisir une solution de télémaintenance conforme à vos obligations légales et aux recommandations de l'ANSSI.

01 — Introduction : La télémaintenance au cœur des enjeux

Un besoin universel, une exigence de conformité croissante

La télémaintenance — ou accès à distance sécurisé — est devenue indispensable pour les équipes IT des organismes publics et des entreprises sensibles. Elle permet d'intervenir rapidement sur les postes de travail, serveurs et systèmes métiers, sans déplacement physique.

Cependant, toute solution de télémaintenance implique des flux de données potentiellement sensibles : identifiants d'accès, données personnelles des agents ou usagers, informations classifiées selon les organisations. Le cadre réglementaire français et européen impose des obligations strictes sur le traitement, le stockage et la transmission de ces données.

■ **67 %** des collectivités utilisent un outil de téléassistance	■■ **43 %** ne vérifient pas la localisation des données hébergées	■ **100 %** des traitements de données doivent être conformes RGPD	■ **NIS 2** entrera en vigueur en France en 2024-25 pour les OIV/OES

Sources : Baromètre SMACL 2023 (collectivités) ; CNIL rapport annuel 2023 — Note : statistiques à titre indicatif issues de rapports publics disponibles

Les 3 questions que tout DSI public doit se poser

- ■ 1. Où sont hébergées les données traitées lors des sessions de télémaintenance ?
- ■ 2. L'éditeur dispose-t-il d'un DPA (Data Processing Agreement) conforme au RGPD ?
- ■ 3. La solution est-elle qualifiée ou certifiée par l'ANSSI, ou a minima auditée ?

■ **Besoin d'un conseil personnalisé ?** Nos experts cloud-store.fr analysent votre contexte et vous recommandent la solution adaptée à votre profil de risque. → cloud-store.fr/contact/

02 — Cadre réglementaire : RGPD, ANSSI et obligations sectorielles

Le RGPD appliqué à la télémaintenance

Le Règlement Général sur la Protection des Données (RGPD, UE 2016/679) s'applique à tout traitement de données à caractère personnel, y compris lors des sessions d'accès à distance. Les obligations clés pour les organismes publics et entreprises sensibles sont :

Obligation RGPD	Application concrète en télémaintenance	Risque de non-conformité
Base légale du traitement	Contrat ou mission de service public documenté	Traitement illicite
DPA avec l'éditeur	Accord écrit sur rôles responsable/sous-traitant	Amende CNIL jusqu'à 4% CA
Transfert hors UE	Vérifier clauses contractuelles types (SCC)	Transfert illicite
Journalisation des accès	Logs horodatés, conservés (durée définie)	Impossibilité d'audit
DPIA si risque élevé	Analyse d'impact obligatoire pour accès sensibles	Mise en demeure CNIL
Droits des personnes	Information des agents sur les accès distants	Réclamation CNIL

NIS 2 et secteur public : nouvelles obligations de cybersécurité

La directive NIS 2 (2022/2555/UE), en cours de transposition en France, étend significativement le périmètre des entités soumises à des obligations de cybersécurité renforcées. Elle concerne notamment les collectivités de taille significative, les établissements de santé, et de nombreuses entreprises fournissant des services essentiels.

Catégorie	Exemples	Obligations clés
Entités essentielles (EE)	OIV, grandes collectivités, hôpitaux, opérateurs télécom	Mesures de sécurité renforcées, audit obligatoire
Entités importantes (EI)	PME secteurs critiques, collectivités moyennes	Mesures proportionnées, déclaration incidents
Chaîne d'approvisionnement	Fournisseurs IT, éditeurs logiciels	Évaluation sécurité des sous-traitants

03 — Les 3 modèles de déploiement expliqués

Comprendre les architectures pour choisir en connaissance de cause

Le modèle de déploiement d'une solution de télémaintenance est le premier critère de conformité. Il détermine où transitent et sont stockées les données, qui en a le contrôle effectif, et quelles certifications sont applicables.

Critère	■ Cloud Éditeur	■ On-Premise	■ Hybride
Souveraineté des données	■ Variable selon hébergeur	✔ Totale maîtrise	✔ Maîtrise partielle
Conformité RGPD	■ Dépend du DPA éditeur	✔ Contrôle interne	✔ Selon configuration
Hébergement France / EU	■ À vérifier contrat	✔ Locaux propres	✔ Possible
Maintenance & updates	✔ Automatique	■ À charge de l'IT	■ Partielle
Coût initial	✔ Faible (abonnement)	■ Investissement CAPEX	■ Mixte
Disponibilité HA	✔ Intégrée	■ À architecturer	✔ Bonne
Audit & logs internes	■ Limités	✔ Complets	✔ Configurables
Qualification ANSSI	■ Rare (SecNumCloud)	✔ Possible	✔ Possible

■ Cloud Éditeur

- Les sessions de télémaintenance transitent par les serveurs de l'éditeur, généralement hébergés dans des datacenters commerciaux.
- Avantage principal : simplicité de déploiement, mises à jour automatiques, disponibilité élevée.
- Point de vigilance RGPD : localisation des données (UE ou hors UE ?), conditions du DPA éditeur, accès éventuel par des tiers (notamment si éditeur américain soumis au CLOUD Act).
- Recommandation : Exiger explicitement l'hébergement en Union Européenne et un DPA conforme signé.

■ On-Premise

- L'infrastructure de télémaintenance est déployée sur les serveurs internes de l'organisme.
- Avantage principal : maîtrise totale des données, pas de dépendance à un cloud tiers, logs internes complets.
- Point de vigilance : nécessite des ressources IT internes pour la maintenance, les mises à jour et la haute disponibilité.
- Idéal pour : OIV, collectivités traitant des données sensibles, organismes soumis à des règles strictes de souveraineté.

■ Hybride

- Combinaison des deux modèles : l'interface de connexion peut passer par un relais cloud, tandis que les données restent sur l'infrastructure locale.
- Avantage principal : flexibilité, bonne balance entre facilité d'usage et contrôle des données.
- Exemple ISL Online : possibilité de déployer un serveur de relais on-premise tout en bénéficiant de l'interface cloud.
- Recommandation : Documenter précisément quels flux passent par le cloud et lesquels restent locaux.

04 — Certifications éditeurs : ce qu'il faut exiger

Le paysage des certifications applicables à la télémaintenance

Face à la multitude de labels et certifications que les éditeurs mettent en avant, il est essentiel de savoir lesquels ont une réelle valeur juridique ou technique dans le contexte français de la commande publique.

Certification / Label	Émetteur	Portée	Pertinence Secteur Public
SecNumCloud	ANSSI	Services cloud	■■■ Recommandé OIV / collectivités
ISO 27001	ISO / Accrédité	SMSI global	■■■ Standard de référence
HDS (Hébergeur Données Santé)	ANS / BSI	Données de santé	■■■ Obligatoire si données patients
SOC 2 Type II	AICPA (US)	Contrôles sécurité	■■ Utile, non suffisant en France
Certification CSPN	ANSSI	Produit logiciel	■■■ Pour logiciels installés
Qualification ANSSI Niveau Standard	ANSSI	Prestataires SSI	■■■ Pour prestataires
GDPR / RGPD DPA contractuel	CNIL / DPO	Données personnelles	■■■ Obligatoire pour tout éditeur

■■ **Point de vigilance :** La certification ISO 27001 est un standard reconnu mais elle ne garantit pas à elle seule la conformité RGPD ni le respect des exigences ANSSI pour les données les plus sensibles. Pour les OIV et les organismes traitant des données de défense ou de souveraineté, seule la qualification SecNumCloud ou CSPN ANSSI offre le niveau de garantie requis. Source : Guide ANSSI "Prestataires de services d'informatique en nuage (SecNumCloud)" — anssi.gouv.fr

Les questions à poser obligatoirement à votre éditeur

- Disposez-vous d'un DPA (Data Processing Agreement) conforme au RGPD, disponible pour signature ?
- Où sont hébergées physiquement les données de session (pays, datacenter, certification HDS si applicable) ?
- Votre solution est-elle soumise à des législations extraterritoriales (CLOUD Act américain, loi sécurité nationale chinoise) ?
- Quelles sont vos certifications de sécurité en cours de validité et vos audits de pénétration récents ?
- Pouvez-vous fournir la liste de vos sous-traitants IT (hébergeurs, CDN, support) ?
- Disposez-vous d'une option de déploiement on-premise ou hybride pour les clients souhaitant conserver leurs données ?

05 — Points de vigilance ANSSI pour les organismes publics

Les recommandations de l'ANSSI sur l'accès à distance

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié plusieurs guides et recommandations directement applicables aux solutions de télémaintenance. Ces recommandations font référence dans les marchés publics IT.

- **Guide ANSSI "Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et logique"**
  Couvre l'authentification pour les accès distants — anssi.gouv.fr
- **Guide ANSSI "Sécurité des accès distants" (PA-022)**
  Recommandations spécifiques pour la configuration des outils de télémaintenance
- **Référentiel SecNumCloud**
  Qualification des prestataires cloud — liste des prestataires qualifiés sur le site ANSSI
- **Référentiel PAMS (Prestataires d'Administration et de Maintenance Sécurisées)**
  En cours de finalisation — cadre pour les prestataires de télémaintenance

Les 8 exigences techniques ANSSI pour la télémaintenance

01	Authentification forte (MFA) obligatoire pour tout accès distant
02	Chiffrement TLS 1.2 minimum pour tous les flux de télémaintenance
03	Journalisation complète et infalsifiable de toutes les sessions
04	Principe du moindre privilège : droits limités aux actions nécessaires
05	Segmentation réseau : isolation du système de télémaintenance
06	Procédure de gestion des incidents documentée et testée
07	Revue régulière des accès et désactivation des comptes inactifs
08	Traçabilité des actions effectuées pendant les sessions (enregistrement vidéo recommandé)

06 — Comparatif des solutions du marché

Cloud-store.fr distribue plusieurs solutions de télémaintenance répondant à différents profils de conformité. Ce comparatif est établi sur la base des informations publiques disponibles au moment de la rédaction. Il ne constitue pas une évaluation exhaustive et les certifications doivent être vérifiées auprès des éditeurs.

Solution	Éditeur	Modèle déploiement	Certifications clés	Hébergement EU	Score conformité*
ISL Online	ISL Online d.o.o.	Cloud / On-Prem / Hybride	ISO 27001, RGPD	Oui (UE)	■■■■
Splashtop	Splashtop Inc.	Cloud	ISO 27001, SOC 2 Type II, RGPD	Oui (UE disponible)	■■■
TeamViewer	TeamViewer SE	Cloud / On-Prem	ISO 27001, SOC 2, RGPD	Allemagne	■■■
BeyondTrust	BeyondTrust Corp.	Cloud / On-Prem	FedRAMP, ISO 27001, SOC 2	Oui (UE)	■■■■
Wallix Bastion	Wallix Group (FR)	On-Prem / Cloud FR	CSPN ANSSI, ISO 27001, CC EAL3+	France	■■■■■

** Score conformité cloud-store.fr établi selon : certifications disponibles, options on-premise, hébergement EU, présence DPA RGPD. Ce score est qualitatif et ne constitue pas une certification officielle.*

ISL Online : la solution référence pour le secteur public français

Parmi les solutions distribuées par cloud-store.fr, ISL Online se distingue par sa flexibilité de déploiement unique : cloud européen, on-premise, ou hybride avec serveur de relais auto-hébergé. Cette architecture permet à chaque organisme public de choisir le niveau de contrôle des données adapté à ses obligations.

✔ **Hébergement EU**	Datacenters en Union Européenne, DPA RGPD disponible
✔ **On-Premise disponible**	Déploiement sur infrastructure interne possible
✔ **Chiffrement end-to-end**	AES 256 bits pour toutes les sessions
✔ **Audit complet**	Journalisation de toutes les actions, export CSV/XML
✔ **Multi-plateforme**	Windows, Mac, Linux, iOS, Android, navigateur
✔ **Authentification**	MFA, SSO, intégration Active Directory

■ **Découvrir ISL Online et Splashtop sur cloud-store.fr** → Solutions de téléaccès : cloud-store.fr → Demander une démonstration : cloud-store.fr/contact/

07 — La checklist du DSI public avant tout déploiement

15 points de contrôle incontournables

Avant de signer tout contrat pour une solution de télémaintenance, le DSI ou RSSI d'un organisme public doit avoir répondu positivement à chacun de ces points.

✔ BONNES PRATIQUES	✘ ERREURS À ÉVITER
✔ DPA éditeur signé et conforme RGPD	✘ Éditeur soumis au CLOUD Act (US) sans mesures compensatoires
✔ Hébergement des données en UE confirmé par contrat	✘ Pas de DPA ou DPA incomplet
✔ Authentification MFA obligatoire pour tous les accès	✘ Authentification par simple mot de passe uniquement
✔ Journalisation complète activée et auditée	✘ Absence de logs de session exploitables
✔ Chiffrement TLS 1.2+ et AES 256 en session	✘ Données stockées hors UE sans garantie contractuelle
✔ Politique de rétention des logs définie	✘ Sous-traitants non déclarés dans le DPA
✔ Procédure de notification de violation documentée	✘ Pas d'option de déploiement on-premise pour les données sensibles
✔ Formation sécurité pour les utilisateurs prévue	✘ Pas de réponse aux incidents documentée

Checklist marché public : clauses à insérer dans vos CCTP

Clause de localisation des données : "Les données à caractère personnel traitées dans le cadre du présent marché devront être hébergées exclusivement au sein de l'Union Européenne."

Clause de sous-traitance : "Le titulaire devra informer le pouvoir adjudicateur de tout recours à un sous-traitant pour le traitement de données personnelles et obtenir son accord préalable."

Clause de sécurité : "Le titulaire devra fournir annuellement un rapport d'audit de sécurité réalisé par un tiers indépendant (PASSI qualifié ANSSI recommandé)."

Clause de réversibilité : "Le titulaire devra garantir la récupération complète des données dans un format exploitable, dans un délai de 30 jours après résiliation du contrat."

08 — Cloud-store.fr : votre partenaire de confiance

Pourquoi choisir cloud-store.fr pour vos solutions de télémaintenance ?

Cloud-store.fr est un distributeur spécialisé en solutions logicielles B2B pour le secteur public et les entreprises sensibles. Notre expertise sur les enjeux de conformité RGPD, de cybersécurité et de commande publique nous permet d'accompagner nos clients au-delà du simple acte d'achat.

■ Expertise sectorielle

Connaissance approfondie des contraintes réglementaires du secteur public français : RGPD, ANSSI, commande publique, CCTP.

■ Sélection rigoureuse

Nous ne distribuons que des solutions dont nous avons vérifié la documentation de conformité : DPA, certifications, hébergement.

■ Accompagnement continu

De l'évaluation initiale au déploiement et au renouvellement, nos équipes restent disponibles pour tout questionnement de conformité.

■ Interlocuteur unique

Un seul contact pour gérer votre portefeuille de licences, vos questions de conformité et vos évolutions de contrat.

■ Aide aux marchés publics

Nous vous aidons à rédiger les clauses techniques de vos CCTP et à évaluer les offres en réponse à vos appels d'offres.

■ Solutions souveraines disponibles

Pour les besoins les plus sensibles, nous proposons des options de déploiement on-premise et des solutions d'éditeurs européens certifiés.

■ Passez à l'action : contactez nos experts

Nos consultants analysent gratuitement votre contexte réglementaire et vous proposent la solution de télémaintenance la mieux adaptée à vos obligations de conformité.

■ cloud-store.fr/contact/

Ou découvrez directement nos solutions :

■ cloud-store.fr

Disclaimer : Ce livre blanc est fourni à titre informatif. Les certifications et informations relatives aux éditeurs cités sont basées sur les sources publiques disponibles au moment de la rédaction (2025) et peuvent évoluer. Cloud-store.fr recommande de vérifier directement auprès des éditeurs la validité et le périmètre de leurs certifications avant tout engagement contractuel. Ce document ne constitue pas un avis juridique.