



**Simon
Uzenat**

SÉNATEUR DU MORBIHAN
Conseiller régional
de Bretagne



Guide pratique à
destination des

Collectivités locales
TPE-PME
Associations
Particuliers



H E X A T R U S T

CLOUD CONFIDENCE & CYBERSECURITY

« **SOUVERAINETÉ NUMÉRIQUE :** **DES SOLUTIONS CONCRÈTES POUR PASSER DE LA PAROLE AUX ACTES !** »

*Des solutions françaises et européennes existent :
efficaces, fonctionnelles, sécurisées, souveraines
et compétitives, elles répondent à vos besoins,
à vos attentes et à vos usages pour aujourd'hui
et pour demain.*

*Dans la continuité des
travaux transpartisans
adoptés à l'unanimité
par la commission
d'enquête du Sénat sur
la commande publique*



↳
Consulter
le rapport



**Edition
2026**

ÉDITO

Simon UZENAT

Sénateur du Morbihan, Président de la commission d'enquête sénatoriale sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française



Dans un contexte géopolitique extrêmement tendu, la dépendance française et européenne à l'égard des solutions numériques étrangères, notamment américaines, induit des risques considérables pour notre sécurité collective, notre autonomie stratégique et nos libertés fondamentales. En effet, le Foreign Intelligence Surveillance Act (Fisa) et le Clarifying Lawful Overseas Use of Data (Cloud) Act permettent au gouvernement des États-Unis d'exiger de sociétés assujetties à la loi américaine la communication des données qu'elles stockent, et ce sans en demander l'autorisation ni même en informer leurs propriétaires (quand bien même les données seraient physiquement hébergées en Europe). Du reste, la Chine et l'Inde ont également adopté des législations similaires.

Lors d'une audition organisée en 2025 par la commission d'enquête sénatoriale, le directeur des affaires publiques et juridiques de Microsoft France, invité à garantir que les données des citoyens français hébergées par Microsoft ne seront jamais transmises à des autorités étrangères sans l'accord des autorités françaises, a clairement répondu : « Non, je ne peux pas le garantir ».

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), l'a quant à lui rappelé avec force devant la commission d'enquête : contre les législations extraterritoriales, il n'existe ni contre-mesures techniques ou contractuelles efficaces. Dans le premier cas, ni le chiffrement, ni la localisation, ni l'anonymisation des données « ne rendent (...) impossible la captation des données en vertu du droit applicable ». Dans le second cas, « un prestataire américain ou chinois qui promettrait de ne jamais communiquer vos données à une autorité de son pays – qu'il s'agisse d'un juge ou d'un service de renseignement – vous promettrait en fait d'aller en prison à votre place ».

Les dangers s'avèrent donc multiples, pour nos organisations publiques et privées, comme pour nos concitoyens : des pressions pourraient être (et ont déjà été) exercées soit par l'utilisation malintentionnée des données obtenues par un gouvernement étranger, soit par la restriction de l'accès à des solutions numériques dont nous sommes encore très largement dépendants (sans compter les hausses de prix subies par des « clients captifs »).

Heureusement, des solutions françaises et européennes existent ! Efficaces, fonctionnelles, sécurisées, souveraines et compétitives, elles répondent aux besoins, aux attentes et aux usages d'aujourd'hui et de demain. Alors que les données (publiques, économiques ou personnelles), sont devenues le nouvel actif stratégique par excellence, il y a désormais urgence à les protéger durablement en faisant confiance à des opérateurs français et européens.

Tel est l'objectif de ce guide opérationnel, conçu en partenariat avec Hexatrust dont je remercie chaleureusement les équipes. Traduction concrète des travaux et recommandations de la commission d'enquête sénatoriale, il vous permettra de mieux connaître ces acteurs robustes et agiles, qui pourront, grâce à votre engagement, œuvrer chaque jour encore davantage à renforcer la souveraineté numérique, économique et démocratique, de notre pays et de notre continent.

LE MOT DU PRÉSIDENT

Jean-Noël DE GALZAIN

Président Hexatrust

Founder & CEO WALLIX Group



La transformation numérique de votre organisation est une réalité incontournable. Chaque jour, vos services traitent des données sensibles concernant vos administrés ou vos clients, vos marchés et vos décisions. La question n'est plus de savoir si vous devez numériser, mais avec quels outils, et selon quelles règles.

Depuis plusieurs années, les uns et les autres se sont massivement tournés vers des plateformes américaines – pour leur simplicité, leur accessibilité, leur prix apparent. Mais derrière cette commodité se cache une réalité juridique et stratégique que chacun doit connaître : le Cloud Act américain de 2018 autorise les autorités américaines à accéder aux données stockées par des entreprises américaines, y compris en Europe, et le FISA 702 permet une surveillance étendue sans contrôle judiciaire préalable.

En tant qu' élu, agent ou chef d'entreprise, vous êtes garant de la protection des données de vos administrés ou clients. En tant qu'acheteur public et privé, vous pouvez orienter vos marchés vers des solutions qui respectent le droit européen, renforcent notre tissu économique et préservent notre capacité de décision collective.

En concertation avec le sénateur Simon Uzenat et dans la continuité des travaux transpartisans de la commission d'enquête sur la commande publique qui ont notamment permis de mettre pleinement en lumière les enjeux de souveraineté numérique, ce guide a été conçu pour vous. Il répond aux idées reçues les plus fréquentes, présente des cas d'usage concrets et vous donne les clés pour passer à l'action dès aujourd'hui. Des alternatives souveraines existent, elles sont performantes, certifiées, et prêtes pour vos besoins.

Pour anticiper vos prochains renouvellements de contrats, voici un guide qui vous permettra de choisir une solution à la fois performante et respectueuse de nos règles et de nos usages... et de participer, vous aussi, à la construction d'un numérique plus souverain !

H E X A T R U S T

CLOUD CONFIDENCE & CYBERSECURITY

À propos d'Hexatrust : Hexatrust réunit plus de 165 entreprises françaises et européenne du numérique de confiance Ensemble, nous offrons des alternatives crédibles, performantes, souveraine et innovantes.



Pourquoi ce guide ?

Votre organisation utilise peut-être des solutions informatiques non souveraines pour ses outils de messagerie, de visioconférence, de partage des fichiers ou encore pour ses signatures électroniques. Mais le choix de ces outils, loin d'être anodin, peut être lourd de conséquences.

Heureusement, des solutions françaises et européennes, crédibles, opérationnelles et ergonomiques existent pour répondre à l'ensemble de vos besoins.

Bien sûr, il n'est pas nécessaire de tout remplacer immédiatement, l'objectif est de pouvoir réduire progressivement ses dépendances. Notre conseil : commencez petit. Identifiez un premier usage – par exemple la visioconférence, la signature électronique ou le partage de fichiers – puis comparez les solutions souveraines disponibles.

Ce guide présente de manière simple et transversale les principales alternatives souveraines pour toutes les organisations, quelle que soit leur taille.



NOTRE CONSEIL

Commencez petit. Identifiez un premier usage !
Par exemple la visioconférence, la signature électronique ou le partage de fichiers, puis comparez les solutions souveraines disponibles.



Sommaire

PARTIE I - IDÉES REÇUES VS RÉALITÉ	P.6
PARTIE II - CARTOGRAPHIE DES ACTEURS	P.9
PARTIE III - CAS D'USAGES	P.13
RESSOURCES ET OUTILS	P.21



PARTIE I

IDÉES REÇUES VS RÉALITÉ



Préjugé n°1 « Les solutions européennes sont inadaptées »

FAUX

Une communauté de communes de 40 agents gère ses agendas et ses documents sensibles avec une solution française, à coût attractif.

La communauté de communes Mont-Lozère n'avait pas besoin d'une suite collaborative avec des centaines de fonctionnalités comme le proposent les acteurs dominants du marché. Elle avait besoin d'emails fiables, d'agendas partagés, d'un espace cloud pour partager des documents sensibles, et d'une administration simple pour une équipe informatique réduite. Elle a choisi Mailo Premium — solution française, données hébergées en France, déployée sans complexité.

Résultat : une administration centralisée depuis un seul espace, des agendas partagés opérationnels pour l'ensemble des 40 agents, et un coût adapté aux moyens d'une petite collectivité. Ni surdimensionné, ni sous-fonctionnel.

Selon le Cigref (2021), 75 % des entreprises utilisent moins de 50 % des fonctionnalités de leur suite collaborative. Payer pour une offre de service surdimensionné n'est pas un gage d'adéquation — c'est souvent l'inverse. L'enjeu n'est pas d'avoir le plus de solutions possibles, mais d'aligner l'outil sur les usages réels.

Les solutions françaises et européennes seraient inadaptées ? Non. Simplement calibrées sur l'usage plutôt que sur le catalogue.



Préjugé n°2 « Changer d'outils coûterait trop cher et prendrait trop de temps »

FAUX

La ville de La Courneuve a divisé sa facture par trois sans rupture de service.

En 2020, la ville de La Courneuve (1 200 agents) déploie la suite Office 365 de Microsoft en urgence pour assurer la continuité d'activité pendant la crise COVID. Quelques mois plus tard, le constat est sans appel : la trajectoire tarifaire est incompatible avec les contraintes budgétaires de la collectivité. La ville engage alors une migration vers BlueMind, via l'intégrateur (installateur) FactorFx.

Résultat : une migration automatisée des emails, agendas et contacts, une coexistence des deux systèmes pendant la transition — sans aucune rupture de service — et, selon la DSI « un coût divisé par trois ».

Les acteurs dominants pratiquent une logique de prix d'entrée attractifs, puis hausses tarifaires imposées au renouvellement, sans alternative réelle. Le coût total de la dépendance va ainsi bien au-delà de la première facture — il englobe des augmentations annuelles non maîtrisées et une perte progressive du pouvoir de négociation face à un fournisseur unique. Les solutions européennes offrent, à l'inverse, des conditions contractuelles équilibrées, une prévisibilité budgétaire sur le long terme, et une immunité juridique aux lois extraterritoriales.



À RETENIR !

- > Analyser ses coûts et anticiper les risques et évolutions non maîtrisées.
- > Reconsidérer l'ouverture à une pluralité de fournisseurs.





Préjugé n°3 « Les solutions françaises ne peuvent pas coexister avec nos outils actuels »

FAUX



La Fédération des Hôpitaux Vaudois (FHV) pilote 12 000 professionnels de santé sur 150 sites — avec Microsoft en coexistence.

La FHV gérait un écosystème fragmenté : des milliers d'utilisateurs, des dizaines d'établissements aux besoins distincts, des outils disparates, et des exigences maximales en matière de souveraineté des données de santé.

Le besoin : rationaliser le recours aux multiples solutions existante.

La réponse : Jalios Workplace, déployé comme socle unifié de l'ensemble des solutions existantes.

Résultat : 800+ espaces collaboratifs actifs. Pas de remplacement brutal, pas de rupture : une intégration fluide, y compris avec l'existant Microsoft.



À RETENIR !

- > Favoriser la coexistence de plusieurs fournisseurs afin de réduire la dépendance.
- > Retenir comme critères principaux l'interopérabilité, l'ouverture et la réversibilité lors du choix d'une solution.



Préjugé n°4 « Les agents ne voudront pas changer d'outils »

FAUX



Le changement est possible lorsqu'il est progressif.

En 2015, Hypoport décide de faire de l'auto-organisation un principe directeur pour l'ensemble de son écosystème. Le défi n'est pas technique : c'est un changement de culture à grande échelle, sur 20 filiales indépendantes aux fonctionnements distincts.

La solution retenue est Talkspirit, déployée non pas comme un simple outil de messagerie, mais comme le système opérationnel de l'organisation.

La méthode : une phase pilote au niveau du comité de direction, puis une généralisation progressive appuyée sur des coachs internes et un dispositif de formation dédié.

Résultat : les filiales engagées disposent d'une vision partagée, savent qui fait quoi, et peuvent faire évoluer leur fonctionnement de manière autonome et structurée. Clarté opérationnelle, responsabilisation, efficacité renforcées.

Ce qui a fonctionné chez Hypoport, c'est la méthode, pas la contrainte.



À RETENIR !

- Mettre en place une méthodologie de conduite du changement avec soutien du COMEX.

La réticence au changement est légitime, mais rarement définitive. La clé n'est pas de forcer l'adoption, mais de la construire. Les acteurs Hexatrust intègrent cette logique d'accompagnement dès la conception.

Préjugé n°5 « Pour nos données sensibles, il vaut mieux rester chez les grands acteurs »

FAUX

L'Assemblée nationale confie plus d'un million de documents parlementaires à une solution française — parce qu'elle ne peut pas faire autrement.

Depuis 2017, les 577 députés, leurs collaborateurs et les services de l'Assemblée nationale travaillent sur la **Suite Wimi** : drive, docs, tâches, visioconférence, messagerie. Le critère déterminant n'était pas le prix ni l'ergonomie, c'était l'impossibilité juridique de confier des travaux parlementaires à un prestataire soumis au droit américain. La solution centralise les projets, cloisonne strictement les équipes parlementaires et protège plus d'un million de documents sensibles. **Pour les données sensibles, la question n'est pas « est-ce sécurisé ? » mais « par quel droit ? »**



À RETENIR !

- Analyser les risques induits par les lois extraterritoriales, notamment en termes de guerre économique.



Préjugé n°6 « La préférence européenne n'a pas d'impact économique et sociétal »

FAUX

Quai des Notaires a remplacé sa solution américaine de signature électronique par Yousign — un acte de souveraineté qui est aussi un acte économique.

Quai des Notaires fournit des outils numériques aux professions réglementées. Quand leur solution américaine de signature électronique est devenue incompatible avec leurs objectifs de souveraineté, ils n'ont pas cherché un équivalent fonctionnel, ils ont cherché un partenaire français.

Leur choix s'est porté sur Yousign : hébergement en France, conformité réglementaire et co-construction avec les équipes Yousign.

Résultat : une plateforme sécurisée qui renforce la confiance des notaires et de leurs clients..

Ce choix individuel s'inscrit dans un enjeu collectif massif. Au-delà de l'emploi, choisir européen, c'est préserver des compétences critiques et la capacité d'innovation sur le territoire, réduire l'empreinte carbone liée aux infrastructures lointaines, favoriser des relations clients-fournisseurs transparentes et équilibrées.

Choisir une solution européenne n'est pas un acte militant. C'est un acte stratégique avec des effets économiques, industriels et géopolitiques mesurables.



À RETENIR !

- Participer à une forme de solidarité économique en orientant les achats vers l'écosystème européen.
- Contribuer à la défense des valeurs européennes : Résilient, Responsable, Réversible, Réciproque, Respectueux de la vie privée.



PARTIE II

CARTOGRAPHIE DES ACTEURS

CYBER PANORAMA BY

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

CESIN

catégorie « **PROTÉGER** ».



VISIOCONFÉRENCE

BlueMind

leviia

] pexip [



PRIVATE
DISCUSS



TIXED



MESSAGERIE
INSTANTANÉE

Jalios

leviia

Olvid



PRIVATE
DISCUSS

Sharekey



TIXED



talkspirit



BlueMind



Jalios



leviia

∞drive



Sharekey

WIMI



STOCKAGE PARTAGE
CO-ÉDITION



Datasure
Certificate authority



PARSEC



PRIVATE
DISCUSS



NetExplorer



Jamespot



Sharekey

∞drive



TIXED

WIMI



Bonnes pratiques contractuelles

En tant qu'acheteur public ou privé, vous disposez de leviers juridiques concrets pour intégrer la résilience numérique dans vos marchés dès lors que cette question est anticipée. Cette liste n'est pas exhaustive mais permet d'identifier des points juridiques clés. Elle ne remplace pas l'avis d'un juriste sur votre marché en particulier et/ou celui des personnes référentes au sein de votre organisation en matière de protection des données et de cybersécurité.

THÉMATIQUE	RISQUE IDENTIFIÉ	BONNES PRATIQUES CONTRACTUELLES
Souveraineté	Accès extraterritorial : lois étrangères (USA, Chine...) permettant l'accès à des données publiques sensibles.	Définir dans le cahier des charges des exigences portant sur la localisation des données, la chaîne de sous-traitance, le droit applicable et les conditions d'accès aux données. Lorsque la sensibilité des données le justifie, exiger que les conditions techniques et juridiques du service limitent leur exposition aux législations étrangères.
Sécurité	Violation de données	Prévoir des exigences de sécurité techniques auditables, au moyen le cas échéant de certifications et des accords conformes à la réglementation sur les données personnelles
Évolution du service	Changements unilatéraux de la part du fournisseur	Prévoir que toute modification substantielle des conditions contractuelles, des conditions de sécurité ou de la localisation des données doit être soumise aux règles de modification du marché et, lorsque cela est nécessaire, faire l'objet d'un accord formalisé.
Qualité de service	Indisponibilité du service	Fixer des niveaux de services stricts : taux de disponibilité (ex : 99,9%/jour ou semaine – en fonction de l'outil), temps de rétablissement (GTR) en quelques heures. Associer ces seuils à des pénalités financières automatiques.
Contrat en cours Interopérabilité	Monopole de fait : le fournisseur verrouille son écosystème, obligeant l'organisation à acheter toute sa suite logicielle.	Découper le marché en lots séparés si possible, intégrer dans les critères d'attribution du marché un sous-critère valorisant l'interopérabilité et l'absence de verrouillage. Imposer contractuellement la mise à disposition d'API ouvertes, documentées et gratuites. Garantir le droit pour l'organisation de connecter des briques tierces (fournisseurs concurrents).
Fin de contrat Réversibilité	Coûts cachés : le prestataire facture des frais pour rendre les données ou traîne à s'exécuter.	- Définir un plan de réversibilité dès la passation du marché. Fixer à l'avance les coûts de sortie (idéalement forfaitaires ou gratuits) et le délai maximal de restitution; - Prévoir la restitution des données dans des formats ouverts, structurés et interopérables.
Fin de contrat Portabilité	Rupture de service : interruption de l'action privée ou publique (ex : état-civil) pendant le transfert vers le repreneur.	Prévoir une clause d'assistance à la portabilité. Le prestataire sortant doit maintenir le service et coopérer avec le repreneur jusqu'à la bascule complète.



PARTIE III

CAS D'USAGES

**Pour chaque outil américain couramment
utilisé dans vos services, des alternatives
souveraines existent.**

Cas 1 – Messagerie et suite bureautique

Vous utilisez aujourd'hui

- Microsoft 365 ;
- Outlook ;
- SharePoint.

Alternatives souveraines

- **BlueMind** : Suite email/agenda/contacts
- **Mailo** : Messagerie professionnelle française,
- **Wimi** : Plateforme collaborative complète
- **Jalios** : Suite collaborative française

Bon réflexe : ne choisissez pas forcément la solution qui propose le plus de fonctionnalités. Choisissez celle qui répond le plus à vos besoins immédiats.

Cas 2 – Visioconférence

Vous utilisez aujourd'hui

- Zoom
- Microsoft Teams ;
- Google meet

Alternatives souveraines

- **Tixeo** : Visio chiffrée de bout en bout
- **Pexip** : Solution européenne (Norvège) de visioconférence, interopérable, haute sécurité
- **Private Discuss** : Visio chiffrée française

Cas 3 – Stockage et partage de fichiers

Vous utilisez aujourd'hui

- Google Drive ;
- OneDrive ;
- WeTransfer;
- Dropbox.

Alternatives souveraines

- **Voltn** : Stockage et partage de fichiers
- **Oodrive** : Plateforme collaborative complète
- **Leviia** : Stockage cloud français, prix compétitif
- **Parsec** : Chiffrement de bout en bout pour fichiers sensibles
- **Wimi** : Plateforme collaborative complète

Bon réflexe : évitez d'envoyer des documents sensibles avec un service grand public sans avoir vérifié où ils sont stockés et qui peut y accéder.

Cas 4 – Messagerie instantanée sécurisée

Vous utilisez aujourd'hui

- WhatsApp
- Telegram
- Microsoft Teams ;

Alternatives souveraines

- **Olvid** : Application de messagerie chiffrée
- **Private Discuss** : Messagerie sécurisée pour équipes, hébergement France
- **Talkspirit** : Réseau social d'entreprise français avec messagerie sécurisée

Bon réflexe : votre téléphone est pratique, mais les applications grand public ne sont pas conçues pour les besoins d'une collectivité.

Vous utilisez aujourd'hui

- DocuSign ;
- Adobe Sign

Alternatives souveraines

- **Yousign** : Signature électronique qualifiée , hébergée en France
- **Docaposte** : Filiale La Poste, solutions certifiées pour le secteur public

Bon réflexe : toutes les signatures électroniques n'ont pas la même valeur juridique ni le même niveau de sécurité - vérifiez que le niveau de signature proposé correspond bien à vos besoins.

Cas 6 – Intelligence Artificielle

Vous utilisez aujourd'hui

- ChatGPT ;
- Copilot ;
- Gemini ;
- Anthropic.

Alternatives souveraines

- **Solutions IA souveraines** : Basées sur Mistral AI (France) ou autres modèles européens,
- **Jamespot / Wimi / Jalios** : Intègrent des assistants IA souverains dans leurs plateformes

Bon réflexe : Avant de donner un document à une IA, posez-vous une question simple : « Est-ce que je transmettrais ce document à une entreprise extérieure ? ». Si la réponse est non, ne le transmettez pas à une IA sans avoir vérifié ce qu'elle fait de vos données.



Comment choisir ?

Cartographie des solutions souveraines Hexatrust

Pour chaque outil américain couramment utilisé dans vos services, le tableau ci-contre indique les solutions membres Hexatrust qui constituent une alternative.

	BlueMind	Datasure	Docaposte	Jalios
TAILLE DE CLIENTS				
Moins de 10		X	X	
10 à 50	X	X	X	
50 à 200	X	X	X	
200 à 1.000	X	X	X	X
1.000 à 5.000	X	X	X	X
5.000 à 100.000	X	X	X	X
Plus de 100.000	X	X	X	X
COUVERTURE FONCTIONNELLE				
Suite bureautique et coédition (Microsoft, Google)		x	X	x
Visio (Zoom, Teams, Meet)	X		X	x
Mail (Outlook/Exchange, Google mail)	X		X	x
Stockage de fichier (WeTransfer, Google Drive OneDrive)	X	x	X	X
Gestion documentaire (Sharepoint)		x	X	X
Réseau Social (Facebook)			X	X
Messagerie instantanée (Whatsapp, Teams)			X	X
Intelligence artificielle (Copilot, ChatGPT)	X		X	x
Signature Electronique (DocuSign, Universign)		X	X	x
Site Intranet (Sharepoint)			X	X

Vous n'avez pas besoin d'être un spécialiste.

Avant de choisir, posez vous simplement ces 6 questions.

1. Où sont stockées les données ?

Demandez à votre fournisseur dans quel pays sont hébergées les données.

2. Quel droit s'applique au fournisseur ?

Un fournisseur peut être juridiquement établi en France tout en appartenant à un groupe soumis à un droit étranger ;

3. Qui peut y accéder et dans quelles circonstances ?

Jamespot	Mailo	Olvid	oodrive	Parsec	Pexip	PrivateDiscuss	Tixeo	Voltn	Wimi	Yotrust
	X	X						X	X	X
	X	X		X		X		X	X	X
X	X	X			X	X	X	X	X	X
X	X	X	X	X		X	X	X	X	X
X	X	X	X	X		X	X	X	X	X
X	X	X	X	X		X	X	X	X	X
X	X		X	X		X	X		X	X
x	x		X	X		x		x	x	
x	x		X		X	X	X		x	
X	X								x	
X	X	X	X	X		X	X	X	X	
X		X	X	X		X	X	X	X	
X						X			X	
X		X	X			X	X		x	
X						X			x	X
x			X			x		x	x	
X										

Légende

Composant de l'éditeur

Composant intégré par l'éditeur

Composant non fourni en standard

X

x

4. Que se passe-t-il opérationnellement ?

(portabilité/interopérabilité) si vous souhaitez changer de fournisseur ou bien installer ultérieurement une solution numérique complémentaire à celle déjà installée ? Vous devez pouvoir quitter une solution facilement, sans perdre vos données ;

5. Avez vous le sentiment de maîtriser le coût de votre contrat ? ;

6. Est-ce que votre choix respecte bien le cadre réglementaire applicable aux administrations publiques ?

BlueMind est une solution complète de messagerie collaborative. Française, souveraine et open source, BlueMind est nativement compatible avec Outlook et tous les autres applicatifs de messagerie (Thunderbird, webmail, mobiles), ce qui permet d'opérer des migrations sans rupture depuis Microsoft. BlueMind compte plus de 500 clients dans les secteurs public (ministère de l'Intérieur, INSEE, villes comme Marseille, Nanterre, Tarbes, Istres,... collectivités territoriales, hôpitaux, SDIS) et privé (Thales, Airbus Defence & Space, Institut Pasteur, INSA Toulouse, PME et grands groupes industriels, IT, transport, aéronautique, services).

Datasure

Autorité de certification française qualifiée par l'ANSSI, Datasure est le seul prestataire de services de confiance qualifié eIDAS à proposer une solution de signature 100% souveraine avec infrastructure sous-jacente multi-secnumcloud. Prévu particulièrement pour les éditeurs de logiciel, l'offre SecuSign API Expert délivra tous les niveaux de signatures (simples, avancés, qualifiés) directement en marque blanche intégré dans l'application cliente. Datasure compte parmi ses références clients publiques et privées le musée du Louvre, Index Éducation (Pronote), Bolloré SE, Paragon et Alice & Bob.

DOCAPOSTE

Filiale numérique du groupe La Poste et référent de la confiance numérique, Docaposte accompagne entreprises et institutions publiques dans leur transformation digitale. Éditeur de solutions de confiance, intégrateur et opérateur de plateformes, elle conçoit et opère des parcours numériques sécurisés et centrés sur l'expérience utilisateur, alliant cloud, cybersécurité et IA.

Docaposte accompagne plus de 60 000 clients, dans l'objectif d'allier souveraineté technologique et intérêt général au service de nos entreprises et des territoires. Ses références incluent notamment des Ministères, France Travail, le CROUS, Orange, La Banque Postale ainsi que plusieurs milliers de collectivités et d'autres établissements publics dans les territoires bretons (EPSM Morbihan, CPAM d'Ille-et-Vilaine, la mairie de Vannes...)

JALIOS

50 organisations de l'administration centrale (DGFIP, Ministère de la Justice, Sénat...),
7 régions (Bretagne, Ile de France...),
49 départements et SDIS (Finistère, Ile-et-Vilaine, Loire-Atlantique,
40 villes ou agglomérations (Nantes Métropole, Saint Nazaire, Communauté de Saint Briec...)
et aussi PME, ETI et grands comptes de tous secteurs (MAIF, Crédit Agricole, Magasins U, Intersport, Terrana, Indigo, Institut Pasteur, CEA, CNRS, Handicap International, Fédération Française de Football...)

Jamespot

Première solution collaborative Certifiée Numérique France Garanti, certifiée ISO 27001, avec 350 organisations clientes et plus de 400 000 utilisateurs en France et à travers le monde, Jamespot accompagne aussi bien des entreprises privées que de grandes administrations publiques et des structures associatives

Messagerie française, compte parmi ses références ATD16 (collectivités), le moteur de recherche Lilo, le registre .Bzh et le Groupe ISARA ISEMA.

oodrive

Oodrive, éditeur de logiciel français, développe des solutions SaaS de collaboration sécurisée pour les données sensibles, au sein d'environnements souverains. Depuis plus de 25 ans, l'entreprise accompagne les organisations dans la gestion et le partage de leurs informations critiques, au cœur des enjeux de sécurité, de conformité et de souveraineté numérique. Ses solutions, qualifiées SecNumCloud 3.2 par l'ANSSI et certifiées ISO 27001/27701 et HDS v2 (Hébergeur de Données de Santé), répondent aux principales réglementations européennes, dont NIS2, DORA et le RGPD. Oodrive compte plus de 3 500 clients : grands groupes, acteurs publics et organisations sensibles. www.oodrive.com

Olvid

La messagerie instantanée Olvid garantit un niveau de sécurité sans précédent. Seule messagerie certifiée par l'ANSSI et recommandée par la DGSI, Olvid garantit mathématiquement l'impossibilité pour un tiers de prendre connaissance des communications. La sécurité ne repose plus sur les serveurs mais sur des protocoles cryptographiques d'excellence. Rupture technologique totale, vous ne cédez absolument aucune donnée à l'éditeur du service, les données restent entre les utilisateurs. Pas d'usurpation d'identité, pas de fuite de données, pas de spam, pas d'espionnage possible, pas de soumission à des lois extra-territoriales et une poursuite des communications même en cas d'attaque informatique. Olvid est utilisé par la Présidence de la République, le Ministère de l'intérieur, le Ministère des armées, le Conseil de l'Europe, Cap Gemini, Sopra Steria, Veolia.

PARSEC Trust the Cloud

PARSEC est un éditeur logiciel français spécialisé dans la protection des données, proposant des solutions SaaS et On-Premise. S'appuyant sur la technologie ZeroTrust, PARSEC garantit la sécurité des échanges collaboratifs tout en assurant la conformité réglementaire du stockage des données. Ses références s'appuient sur de grandes institutions publiques : la Préfecture de Police (5 000 à 100 000 utilisateurs, en déploiement), le Ministère de l'Intérieur (5 000 à 100 000, en évaluation) et le CNRS (5 000 à 100 000, déployé), ainsi que le Groupe Hospitalier de la Vallée du Quercy (10 à 50, déployé) dans le secteur de la santé.

] pexip [

Pexip est le spécialiste européen des solutions de visioconférence souveraines et sécurisées. Pexip accompagne les administrations publiques, Collectivités territoriales, établissements de santé, centres de recherches et d'autres services de l'Etat pour intégrer la visioconférence au cœur de leurs usages quotidiens, en garantissant un haut niveau de sécurité, de protection des données et d'interopérabilité multi-plateformes (Teams, Google, Zoom...). Pexip permet ainsi d'améliorer la qualité de vie au travail des agents, de renforcer la communication interne et inter-administration, mais également de créer de nouveaux services à destination des citoyens (RDV administratifs en vidéo, télé-consultation santé, télé-justice...). Pexip est certifié auprès de l'ANSSI.



Private Discuss est une plateforme française sécurisée de messagerie instantanée, visioconférence, webinaire et collaboration, avec chiffrement de bout en bout et déploiement On-Premise, SaaS ou SecNumCloud. Elle dispose de son propre compagnon IA pour la transcription, la traduction et le résumé de réunions, développé en interne sans service tiers. Private Discuss compte parmi ses références clients le groupe EDF (dont Framatome, Enedis, etc.), JCDecaux, Sodern (ArianeGroup), ou encore le groupe financier italien Azimut, et parmi ses références publiques la Cour des comptes, le ministère des Armées, de la Santé et le Centre national de formation aux crises du ministère de l'Intérieur (CNCMFE).



Tixeo protège les échanges critiques des organisations stratégiques avec sa solution de visioconférence collaborative sécurisée. Sa technologie, certifiée ANSSI, garantit un chiffrement de bout en bout, en cloud comme On-premise. Elle est notamment plébiscitée par le ministère des Armées, KNDS, MBDA, Naval Group, Dassault Aviation, Safran, Orano ou encore Orange.

Voltn

Voltn (anciennement NetExplorer) est l'expert du fichier en entreprise. Stocker, partager, coéditer, signer, valider, tracer, retrouver : l'éditeur couvre tout le cycle de vie du fichier. Depuis plus de quinze ans, il répond à ce besoin avec deux produits : Voltn Share pour échanger avec l'extérieur, Voltn Workspace pour réunir et maîtriser les fichiers de l'entreprise.

2 000 organisations et 300 000 utilisateurs quotidiens lui confient leurs fichiers, soit plus de 500 millions de fichiers à ce jour. L'entreprise, basée à Toulouse, héberge ces fichiers en France ou au Luxembourg. Elle est certifiée ISO 9001, ISO 27001, Hébergeur de Données de Santé (HDS) et labellisée Numérique Responsable (NR).



Wimi est un acteur souverain et sécurisé du travail collaboratif et de la gestion de projet, qualifié SecNumCloud 3.2 SaaS ANSSI. Sa suite collaborative, simple à prendre en main, réunit les briques essentielles à la productivité des équipes, et compte plus de 55 000 clients dans le monde. Dans le Golfe du Morbihan, Wimi équipe Vannes Agglomération (800 agents, collaboratif souverain, migration messagerie prévue en 2027), la Ville de Plescop (messagerie et collaboratif pour 70 agents/élus) et le CDG 56 (partage de documents et Chat pour animer son réseau de Secrétaires Générales de Mairie). En Bretagne, Saint-Malo utilise Wimi Projets pour son service communication (~15 agents), Ouest-France s'appuie sur Wimi Resilience (PCA, ~50 utilisateurs), et le CHU de Brest utilise Wimi Drive pour la collaboration en pharmacie (une dizaine de collaborateurs).



Youtrust (ex Yousign) réunit trois briques : signature électronique, vérification d'identité et de documents, et cachet électronique, utilisables séparément ou orchestrées au sein de parcours intégrés. Avec plus de 30 000 organisations clientes, Youtrust accompagne la transformation numérique en simplifiant des processus qui doivent être clairs, sécurisés et conformes, grâce à une API flexible et facilement intégrable.



Ressources et outils

Pour aller plus loin et accompagner votre démarche de souveraineté numérique.



Hexadiag : diagnostiquez votre maturité numérique

Hexadiag est un outil de diagnostic gratuit qui vous permet d'évaluer en quelques minutes la maturité numérique de votre collectivité et d'identifier les axes prioritaires de souveraineté.

www.hexatrust.com/hexadiag/



HexaSearch : trouvez la solution qui correspond à vos besoins

HexaSearch est un moteur de recherche référent pour trouver des solutions parmi le catalogue nos membres.

www.hexatrust.com/membres/



Mon Aide Cyber

Mon Aide Cyber est un service d'accompagnement en cybersécurité mis en place par l'ANSSI

monaide.cyber.gouv.fr/

**Vous recherchez une solution souveraine ?
Faites-nous remonter vos besoins**



HEXATRUST, 5-7 rue Bellini, 92800 Puteaux

Date de publication : septembre 2026

Les crédits : FIX Illustration - AdobeStock : 1043451562, 1900510512

© 2026 Hexatrust – Tous droits réservés.

Cette publication est diffusée à titre gratuit. Toute reproduction, représentation, adaptation ou diffusion, intégrale ou partielle, par quelque procédé que ce soit, sans l'autorisation préalable écrite de Hexatrust, est interdite.

Pour toute demande d'utilisation ou de reproduction, contacter : Dorothee DECROP, contact@hexatrust.com.

Ne pas jeter sur la voie publique.



Notes



[illegible]

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

ADRESSE

5 rue Bellini
92800 Puteaux

CONTACT

contact@hexatrust.com

www.hexatrust.com



ADRESSE

17 avenue de Verdun
56000 Vannes

15 rue de Vaugirard
75006 Paris

CONTACT

02 97 60 10 74
echangeons@simonuzenat.bzh

www.simonuzenat.bzh