Stratégie, Sécurité

Prestataire web et accès administrateur Comment éviter les dépendances dangereuses

Un site professionnel ne doit jamais dépendre d’un seul prestataire ou d’un seul compte administrateur. Nom de domaine, hébergement, DNS, WordPress, sauvegardes, licences, emails, Search Console : une PME doit savoir qui possède quoi, qui peut intervenir, et comment récupérer ses accès.

Publié le 20 juin 2026

Le risque n’est pas de déléguer, c’est de perdre la maîtrise

La dépendance à un prestataire web ne vient pas seulement d’un contrat. Elle vient surtout des accès : qui possède le nom de domaine, qui contrôle le DNS, qui détient l’hébergement, qui a le compte administrateur WordPress, qui reçoit les alertes, qui possède les licences premium, qui peut restaurer une sauvegarde.

Pour une PME, le risque est opérationnel, commercial, juridique et parfois stratégique. Si un seul prestataire détient tous les accès, l’entreprise peut se retrouver bloquée en cas de conflit, d’indisponibilité, de changement d’agence, de fin de contrat, de cyberattaque ou de simple urgence.

Le bon objectif n’est pas de donner tous les accès à tout le monde. C’est l’inverse : organiser les accès avec méthode. L’entreprise doit rester propriétaire de ses actifs critiques, tout en permettant au prestataire d’intervenir efficacement.

Quand le site appartient techniquement à quelqu’un d’autre

Beaucoup de PME pensent posséder leur site parce qu’elles l’ont payé. En pratique, la question est plus subtile : elles possèdent peut-être le design, les contenus ou le nom commercial, mais pas toujours les accès qui permettent de piloter le site.

Le nom de domaine peut avoir été enregistré sur le compte du prestataire. L’hébergement peut être dans un compte agence. Le DNS peut être géré dans un Cloudflare que le client ne voit pas. Les licences Elementor, sauvegarde, sécurité ou formulaire peuvent appartenir au prestataire. La Search Console peut être au nom d’un ancien freelance.

Tant que tout se passe bien, cette organisation paraît confortable. Le prestataire s’occupe de tout, le client n’a pas à gérer la technique. Mais le jour où il faut intervenir vite, changer d’agence, restaurer le site, transférer le domaine, corriger le DNS ou récupérer les sauvegardes, cette dépendance devient un risque.

Cadre central

Le bon modèle n’est pas “tout garder” ni “tout déléguer” : l’entreprise conserve la propriété et la maîtrise, le prestataire reçoit les accès nécessaires pour administrer.

Notion | Question à poser
Propriété | À qui appartient officiellement l’actif : domaine, compte, licence, hébergement ?
Accès | Qui peut se connecter, avec quel rôle, et jusqu’à quand ?
Administration | Qui gère techniquement l’actif au quotidien ?

Les actifs critiques à ne jamais perdre de vue

Avant de parler d’accès, il faut identifier ce qui a de la valeur. Le prestataire peut administrer ces éléments, mais l’entreprise doit savoir où ils sont, qui les possède, et comment y accéder.

Actif	Pourquoi c’est critique
Nom de domaine	C’est l’adresse officielle du site et souvent des emails.
DNS	Il dirige le site, les emails, SPF/DKIM/DMARC, redirections et sous-domaines.
Hébergement	Il contient les fichiers, bases de données, logs et parfois les sauvegardes.
WordPress	Il permet de gérer contenus, comptes, extensions, thèmes et paramètres.
Base de données	Elle contient les contenus dynamiques, réglages, utilisateurs, commandes.
Sauvegardes	Elles permettent la reprise après erreur, panne ou attaque.
Emails	Ils servent à recevoir demandes clients, alertes, réinitialisations et notifications.
Search Console	Elle signale indexation, erreurs, spam SEO et problèmes de sécurité.
Analytics / Tag Manager	Ils contiennent l’historique de mesure et les balises du site.
Licences premium	Elles conditionnent mises à jour, support et sécurité de certains plugins.
Comptes publicitaires et réseaux sociaux	Ils portent campagnes, audiences, facturation, pixels et historique.

Propriété, accès, administration : trois notions à distinguer

Une confusion fréquente consiste à mélanger propriété et accès. La propriété désigne qui détient officiellement l’actif : titulaire du nom de domaine, propriétaire du compte Google, client de l’hébergeur, détenteur de la licence.

L’accès désigne la capacité à se connecter à un outil. Un prestataire peut avoir un accès administrateur sans être propriétaire du compte. C’est souvent le bon modèle : le client reste propriétaire, le prestataire est invité avec un rôle adapté.

L’administration désigne l’action de gérer au quotidien : mises à jour, configuration, support, sécurité, supervision. Une entreprise peut déléguer l’administration sans perdre la propriété.

Phrase à retenir :

le prestataire peut administrer, mais l’entreprise doit conserver la maîtrise.

Les mauvais schémas qui créent une dépendance

Certaines organisations semblent pratiques au départ, mais deviennent dangereuses. Le problème n’est pas la délégation. Le problème est la délégation sans réversibilité.

Situation	Risque
Domaine enregistré sur le compte personnel du prestataire	transfert difficile, dépendance juridique et opérationnelle

DNS dans un compte que le client ne connaît pas | impossibilité de modifier site, emails ou authentification email
Un seul compte admin WordPress partagé | traçabilité impossible, risque sécurité accru
Licences premium toutes détenues par l'agence | perte de mises à jour ou fonctionnalités en fin de contrat
Sauvegardes stockées uniquement chez le prestataire | reprise bloquée en cas de rupture ou indisponibilité
Search Console au nom d'un ancien intervenant | perte d'alertes SEO et sécurité
Hébergement sans accès client | impossible d'ouvrir un ticket ou d'exporter le site
Pas de procédure de sortie | changement de prestataire conflictuel ou lent
Mots de passe envoyés par email | risque de compromission et absence de gouvernance
Comptes créés avec une adresse personnelle | perte d'accès si la personne quitte l'entreprise

Ce que l'entreprise doit posséder directement

Pour une PME, certains actifs devraient être au nom de l'entreprise ou dans un compte contrôlé par elle. Ce modèle n'empêche pas le prestataire de travailler. Il évite simplement qu'il soit le seul point de contrôle.

Actif | Recommandation
Nom de domaine | titulaire et contact administratif au nom de l'entreprise
Registrar | compte accessible par l'entreprise ou procédure de délégation claire
DNS / Cloudflare | compte entreprise, avec prestataire invité si possible
Hébergement | contrat au nom de l'entreprise ou mandat clairement documenté
Search Console | propriété validée par un compte entreprise
Analytics / Tag Manager | propriété ou accès administrateur entreprise
Adresses emails principales | comptes internes, pas adresses personnelles du prestataire
Sauvegardes stratégiques | copie récupérable par l'entreprise
Licences clés | modèle clarifié : client propriétaire ou licence agence documentée
Comptes publicitaires | propriété entreprise, prestataire invité comme partenaire
Réseaux sociaux | comptes et pages au nom de l'entreprise

Comptes administrateurs WordPress : les bonnes pratiques

WordPress est souvent le cœur opérationnel du site. Les comptes administrateurs doivent donc être gérés avec rigueur. La documentation officielle WordPress rappelle que les rôles définissent ce que chaque utilisateur peut faire dans le site, et qu'il faut donc adapter le rôle au besoin réel.

Bonne pratique	Pourquoi
Un compte par personne	traçabilité des actions
Pas de compte partagé "admin"	impossible de savoir qui a fait quoi
Supprimer les anciens accès	éviter les comptes oubliés
Rôle adapté au besoin	tous les intervenants n'ont pas besoin d'être administrateurs
2FA pour les comptes sensibles	réduire le risque de compromission
Email de récupération maîtrisé	éviter qu'un ancien prestataire récupère le compte
Journalisation si possible	utile en cas d'incident
Revue périodique des comptes	vérifier qui a encore accès

Les rôles WordPress à connaître

WordPress propose par défaut plusieurs rôles. Un prestataire chargé de la maintenance technique peut avoir besoin d'un accès administrateur. Un rédacteur, un partenaire éditorial ou un intervenant contenu n'en a généralement pas besoin.

Rôle WordPress	Usage recommandé
Super Admin	uniquement pour un réseau multisite WordPress ; très rarement nécessaire pour un prestataire classique
Administrateur	maintenance technique, plugins, thème, réglages, utilisateurs ; à réserver aux intervenants de confiance
Éditeur	gestion éditoriale complète : publier, modifier et gérer les contenus, sans accès technique complet
Auteur	rédaction et publication de ses propres articles
Contributeur	rédaction de brouillons sans publication
Abonné	accès simple à un espace privé ou à un profil utilisateur

DNS, domaine et emails : le trio à protéger en priorité

Le nom de domaine et le DNS sont souvent plus critiques que le site lui-même. Si le domaine expire, le site et les emails peuvent tomber. Si le DNS est mal modifié, le site peut pointer au mauvais endroit. Si les enregistrements emails sont cassés, les messages peuvent ne plus arriver ou partir en spam.

Élément	À vérifier

Titulaire du domaine | entreprise, pas prestataire ou personne physique externe
Contact administratif | adresse contrôlée par l'entreprise
Renouvellement | automatique, moyen de paiement, alerte
Accès registrar | disponible, protégé par 2FA
Accès DNS | propriétaire identifié, prestataire invité si possible
SPF/DKIM/DMARC | responsables identifiés pour les emails
Sous-domaines | cartographie des usages : site, app, tracking, formulaires
Redirections | documentées pour éviter les suppressions accidentelles

Point de vigilance ICANN

Selon les règles applicables aux domaines génériques, un registrar peut refuser le transfert vers un autre registrar dans les 60 jours suivant un changement de titulaire ou de certaines informations du titulaire. Certains registrars proposent une option de renonciation à ce verrou, mais pas tous. C'est une raison supplémentaire pour que le domaine soit correctement enregistré au nom de l'entreprise dès le départ.

Licences premium : attention aux licences "agence"

De nombreux sites WordPress utilisent des extensions premium : Elementor Pro, formulaires, SEO, sécurité, sauvegarde, traduction, WooCommerce, cache, galerie, réservation, paiement, etc.

Modèle | Avantage | Risque
Licence client | le client possède la licence | coût et renouvellement à gérer
Licence agence / développeur | le prestataire mutualise une licence multisite | dépendance en fin de contrat

Les licences agence ne sont pas mauvaises en soi. Elles permettent parfois au client de bénéficier d'outils professionnels à moindre coût. Mais le contrat doit préciser ce qui se passe si la relation se termine : maintien temporaire, transfert vers une licence client, remplacement de l'outil, ou perte des mises à jour premium.

Un site ne doit pas découvrir au moment du départ que plusieurs fonctions critiques dépendaient de licences détenues par l'ancien prestataire.

Sauvegardes : l'accès de dernier recours

La sauvegarde est l'assurance opérationnelle du site. Mais elle ne sert à rien si l'entreprise ne peut pas l'obtenir. Le contrat ou la procédure doit préciser les conditions de restauration et de restitution.

Question | Risque si flou
Où sont stockées les sauvegardes ? | impossible de les récupérer en urgence
Qui peut restaurer ? | dépendance à un seul prestataire
Le client peut-il obtenir une copie ? | difficulté à changer d'agence
Quelle fréquence et rétention ? | perte de données ou point trop ancien
Les sauvegardes sont-elles testées ? | restauration incertaine
Les sauvegardes incluent-elles base et fichiers ? | site partiellement restaurable
Que se passe-t-il en fin de contrat ? | perte de l'historique de reprise

Search Console, Analytics et comptes tiers

Les comptes tiers sont souvent oubliés lors d'un changement de prestataire. Pourtant, ils portent une partie importante de l'historique du site. Le bon modèle est de créer les comptes au nom de l'entreprise, puis d'ajouter le prestataire comme utilisateur ou partenaire.

Compte | Pourquoi il compte
Search Console | indexation, erreurs, sécurité, spam SEO
Google Analytics | historique de trafic, objectifs, sources
Tag Manager | pixels, conversions, scripts tiers
Google Ads / Meta Ads | campagnes, audiences, facturation
Brevo / Mailchimp / Mailjet | newsletters, contacts, réputation d'envoi
Stripe / PayPal | paiements, rapprochements, litiges
Outils de support | tickets, demandes clients, historique
CDN / Cloudflare | DNS, cache, sécurité, performance
Outils anti-spam / SMTP | formulaires, délivrabilité, emails transactionnels

Accès prestataire et sous-traitance

Un prestataire web peut accéder à des données personnelles : formulaires, emails, comptes utilisateurs, commandes WooCommerce, logs, sauvegardes, exports CRM, analytics, support client.

Dès lors que le prestataire traite ces données pour le compte de l'entreprise, il est généralement sous-traitant au sens du RGPD. L'article 28 impose un contrat écrit entre le responsable de traitement et le sous-traitant, précisant notamment l'objet, la durée, la nature et la finalité du traitement, les types de données, les catégories de personnes concernées, les obligations de confidentialité, les mesures de sécurité, l'assistance, les sous-traitants ultérieurs et le sort des données en fin de prestation.

Le contrat doit aussi cadrer les sous-traitants ultérieurs. Si le prestataire web utilise lui-même un hébergeur, un CDN, un outil de sauvegarde cloud, une solution SMTP ou un service de sécurité qui traite des données personnelles, il doit respecter les conditions prévues par l'article 28. Le sous-traitant ne peut pas recruter un autre sous-traitant sans autorisation écrite préalable, spécifique ou générale, du responsable de traitement, et il doit l'informer des changements prévus afin de lui permettre d'émettre des objections.

À retenir

Un accès administrateur WordPress peut donner accès à beaucoup plus de données qu'on ne l'imagine. Le sujet RGPD doit donc être traité dans le contrat, pas seulement dans une politique de confidentialité.

Sécuriser sans bloquer le prestataire

L'objectif n'est pas de compliquer le travail du prestataire. Un prestataire doit pouvoir intervenir vite et correctement. Mais les accès doivent être organisés.

- ?créer un compte nominatif pour chaque intervenant ;
- ?utiliser le rôle minimal nécessaire ;
- ?activer l'authentification à deux facteurs sur les comptes sensibles ;
- ?éviter les mots de passe transmis par email ;
- ?utiliser un gestionnaire de mots de passe partagé ;
- ?documenter les accès critiques hors du site ;
- ?limiter les accès temporaires dans le temps ;
- ?supprimer les comptes à la fin de l'intervention ;
- ?conserver un accès administrateur client ;
- ?tester la récupération des comptes stratégiques.

Accès temporaires

WordPress ne propose pas nativement une expiration automatique des comptes temporaires. Pour créer des accès limités dans le temps, il faut généralement utiliser un plugin dédié ou une procédure interne stricte : date de création, date de suppression prévue, responsable du contrôle.

La sécurité ne consiste pas à refuser les accès. Elle consiste à savoir qui a accès, à quoi, pourquoi, et jusqu'à quand.

Changement de prestataire : la clause de réversibilité

La réversibilité est la capacité à sortir proprement d'un contrat ou à changer de prestataire sans perdre le contrôle du site. Elle doit être prévue avant le conflit, pas après.

Élément à restituer	Exemple
Accès WordPress	comptes administrateurs, rôles, emails associés
Accès hébergement	panel, SFTP ou SSH si applicable ; FTP non chiffré à éviter
Accès DNS / domaine	registrar, Cloudflare, zones DNS
Sauvegardes	dernière sauvegarde complète fichiers + base
Licences	état des licences, modèle de propriété, renouvellements
Documentation	plugins critiques, thème, spécificités, cron, intégrations
Comptes tiers	Search Console, Analytics, SMTP, newsletter, paiement
Code spécifique	thème enfant, snippets, développements sur mesure
État technique	versions, alertes, risques connus, tâches en cours

Une clause de sortie claire protège autant le client que le prestataire. Elle évite les accusations, les blocages et les départs désorganisés.

Les erreurs fréquentes

Erreur	Conséquence
Le domaine est au nom du prestataire	l'entreprise ne maîtrise pas son actif principal
Un seul compte admin partagé	aucune traçabilité
Aucun accès hébergement côté client	dépendance totale pour restaurer ou migrer
Licences agence non documentées	perte de mises à jour en fin de contrat
Pas de copie de sauvegarde récupérable	changement de prestataire difficile
Search Console chez un ancien freelance	perte d'alertes critiques
Mots de passe envoyés par email	risque sécurité et absence de gouvernance
Accès anciens jamais supprimés	surface d'attaque inutile
Pas de clause de réversibilité	blocage ou conflit en sortie

Contrat sans article RGPD / DPA | accès aux données personnelles mal encadré

Checklist dirigeant : que vérifier maintenant ?

Question | Si la réponse est floue
Le domaine est-il bien au nom de l'entreprise ? | l'actif principal peut être difficile à récupérer
L'entreprise a-t-elle accès au registrar ? | impossible de gérer renouvellement ou transfert
Qui contrôle le DNS ? | site et emails peuvent être bloqués
Existe-t-il un compte WordPress administrateur client ? | dépendance totale au prestataire
Les comptes admin sont-ils nominatifs ? | aucune traçabilité des actions
Les anciens accès sont-ils supprimés ? | risque de sécurité inutile
Les sauvegardes sont-elles récupérables ? | reprise ou migration incertaine
Les licences premium sont-elles documentées ? | perte possible des mises à jour
Search Console et Analytics appartiennent-ils à l'entreprise ? | perte de données et d'alertes
Un DPA / accord RGPD existe-t-il avec le prestataire ? | sous-traitance mal encadrée
Une clause de sortie est-elle prévue ? | changement de prestataire risqué
Le plan d'accès est-il stocké hors du site ? | inutilisable si WordPress est inaccessible

Méthode simple pour reprendre la maîtrise

- 01Lister les actifsDomaine, DNS, hébergement, WordPress, sauvegardes, emails, licences, Search Console, Analytics, outils tiers.
- 02Identifier les propriétairesPour chaque actif : entreprise, prestataire, ancien prestataire, salarié, compte personnel, compte agence.
- 03Identifier les accèsQui peut se connecter ? Avec quel rôle ? Avec quelle adresse email ? Avec ou sans double authentification ?
- 04Corriger les actifs critiquesPriorité au domaine, DNS, hébergement, sauvegardes et comptes administrateurs.
- 05DocumenterCréer une fiche d'accès hors WordPress : où sont les accès, qui les détient, comment les révoquer, qui contacter.
- 06Sécuriser2FA, gestionnaire de mots de passe, comptes nominatifs, suppression des anciens accès, rôles adaptés.
- 07Prévoir la sortieAjouter une clause de réversibilité, une procédure de restitution et un état technique en fin de contrat.

Ce que les lecteurs demandent souvent

Est-ce normal qu’un prestataire ait un accès administrateur WordPress ?

Oui, s’il assure la maintenance ou intervient techniquement. Mais cet accès doit être nominatif, sécurisé, justifié, et l’entreprise doit conserver son propre accès administrateur.

Le nom de domaine peut-il être chez le prestataire ?

C’est possible, mais ce n’est pas l’idéal. Le titulaire du domaine doit être l’entreprise, et une procédure de transfert ou de délégation doit être prévue. Le domaine est un actif stratégique.

Que faut-il savoir sur le verrou ICANN de 60 jours ?

Après certains changements de titulaire ou d’informations du titulaire, un transfert vers un autre registrar peut être refusé pendant 60 jours. Certains registrars proposent une option de renonciation, mais il vaut mieux éviter d’avoir à corriger ce point dans l’urgence.

Faut-il donner l’accès complet à l’hébergement ?

Pas toujours. Cela dépend du périmètre. Mais si le prestataire doit restaurer, diagnostiquer, consulter des logs ou migrer le site, il lui faudra un accès adapté. L’accès technique doit privilégier SFTP ou SSH ; le FTP non chiffré est à éviter.

Que faire si un ancien prestataire détient encore des accès ?

Il faut commencer par l’inventaire, puis révoquer ou remplacer les accès : comptes WordPress, SFTP/SSH, base de données, Cloudflare, Search Console, Analytics, SMTP, sauvegardes, outils tiers. Il faut aussi changer les mots de passe partagés.

Une licence agence est-elle dangereuse ?

Pas en soi. Elle peut être économique et pratique. Mais le contrat doit dire ce qui se passe en fin de relation : maintien temporaire, achat d’une licence client, remplacement de l’outil ou perte des mises à jour.

Le prestataire doit-il me remettre une sauvegarde ?

Si le contrat le prévoit, oui. C’est précisément pour cela que la clause de restitution est importante. Une PME devrait pouvoir récupérer au moins une sauvegarde complète fichiers + base à la fin du contrat.

Le client doit-il avoir tous les mots de passe ?

Le client doit pouvoir récupérer la maîtrise de ses actifs critiques. Cela ne signifie pas nécessairement diffuser tous les mots de passe à tous les salariés. Un gestionnaire de mots de passe ou un coffre d'accès permet de sécuriser cette organisation.

Comment éviter de bloquer le prestataire ?

En donnant des accès adaptés, documentés et sécurisés : comptes nominatifs, rôles appropriés, 2FA, accès temporaires si besoin, procédure d'urgence. La bonne gouvernance ne ralentit pas le prestataire ; elle évite le chaos.

Déléguer oui, perdre la maîtrise non

Une PME peut parfaitement déléguer la gestion technique de son site web. C'est même souvent nécessaire. Mais déléguer ne doit pas signifier abandonner la maîtrise de ses actifs numériques.

Le domaine, le DNS, l'hébergement, les comptes administrateurs, les sauvegardes, les licences et les outils tiers doivent être connus, documentés et récupérables. Les accès doivent être suffisamment ouverts pour permettre au prestataire de travailler, mais suffisamment organisés pour éviter la dépendance, la perte de traçabilité ou le blocage en cas de changement.

La bonne question n'est donc pas : faut-il faire confiance au prestataire ?La bonne question est : avons-nous organisé cette confiance avec des accès clairs, sécurisés et réversibles ?

Sources

• ANSSI, Maîtriser les risques de l'infogérance : perte de maîtrise, sécurité, responsabilités, sous-traitance et réversibilité.

• CNIL, Sous-traitant : la CNIL publie un guide RGPD : encadrement contractuel de la sous-traitance.

• CNIL, RGPD, chapitre IV, article 28 : obligations du sous-traitant et sous-traitants ultérieurs.

• WordPress.org, Roles and Capabilities : rôles utilisateurs par défaut et capacités associées.

• WordPress Developer Resources, Hardening WordPress : sécurité des accès, permissions, configuration, plugins et thèmes.

• ICANN, Name Holder FAQs : transfert de noms de domaine, changement de titulaire et verrou de transfert.

• Cybermalveillance.gouv.fr : bonnes pratiques, sensibilisation et assistance aux entreprises en cas d'incident cyber.