

DOCUMENTS VENDOCERTA

Sécurité et RGPD

La protection des données dans VendoCerta est répartie dans tout le produit : la façon dont l'historique est écrit, qui peut voir quel document, comment le compte bancaire est chiffré, et ce qu'un rôle ne peut délibérément pas faire. Cette page rassemble tout cela en un seul endroit.

5

rôles à pouvoirs séparés

5

règles qu'aucun rôle ne contourne

AES-256

chiffrement des données sensibles

Six questions qui reviennent en premier.

Les données peuvent-elles rester chez nous ?

Oui. VendoCerta s'installe sur une infrastructure que vous contrôlez.

Comment les données sensibles sont-elles protégées ?

AES-256-GCM au repos ; la divulgation exige un mot de passe ressaisi et un motif enregistré dans l'historique.

Qui a accès à quoi ?

Des rôles avec une réelle séparation des pouvoirs. Personne ne change son propre rôle.

Y a-t-il un second facteur de connexion ?

Oui, obligatoire pour les rôles ayant accès aux données métier.

Une seule personne peut-elle changer le compte bancaire d'un fournisseur ?

Non. Quatre étapes, des rôles séparés, au moins deux personnes.

Peut-on corriger le journal d'audit ?

Non. Aucune fonction d'édition ou de suppression dans l'interface, quel que soit le rôle, même pour le propriétaire.

Une entrée ne peut être ni modifiée ni supprimée. Même par le propriétaire.

Chaque action enregistrée devient une entrée : connexion, changement de statut d'un fournisseur, décision documentaire, invitation envoyée, fichier téléchargé. VendoCerta n'a nulle part de fonction d'édition ou de suppression d'une entrée et n'écrase jamais un événement existant.

Avant et après, à chaque changement de donnée

Chaque entrée porte : qui, quoi, quand — et lors d'un changement, aussi les valeurs des deux côtés.

Les refus sont aussi enregistrés

Si quelqu'un tente d'ouvrir ce pour quoi il n'a pas les droits, cette tentative devient une entrée. Les tentatives répétées sont donc visibles, pas silencieuses.

Une vue filtrée est un lien

Les filtres se répercutent dans l'adresse de la page, ce qui permet de transmettre un extrait précis de l'historique — à un collègue ou un auditeur — sous forme d'adresse.

Une rétention propre — et nous le disons ouvertement

Le nombre de jours en bas de l'écran de l'historique d'audit n'est pas le même champ que celui de l'écran des paramètres. La rétention de l'historique d'audit est un réglage distinct, actuellement non modifiable depuis l'interface, et changer l'autre champ ne l'affecte pas.

La seule opération que le produit refuse de faciliter.

Changer le compte bancaire d'un fournisseur suit quatre étapes et une règle sur qui peut les conclure. Tout le reste dans VendoCerta est conçu pour supprimer la friction ; ceci est conçu pour la conserver.

Chiffré dès l'enregistrement

Le numéro de compte ne réside jamais en clair dans la base — AES-256-GCM au repos, dès l'enregistrement.

La divulgation coûte trois choses

Le droit sur les données sensibles, une nouvelle saisie du mot de passe malgré la connexion active, et un motif enregistré dans l'historique. Le motif est conservé ; le numéro jamais. Le numéro disparaît de l'écran après 45 secondes.

Les doublons sont montrés, pas cachés

Si le même numéro de compte figure déjà chez un autre fournisseur, l'avertissement doit être écarté sciemment avant qu'une approbation ne devienne possible.

Cinq rôles, et celui qui surprend est volontaire.

L'administrateur système maintient l'installation en bon état — configuration, diagnostics, sauvegardes — et n'a aucun accès aux fournisseurs, documents, dossiers ou comptes bancaires. Exactement l'inverse de l'administrateur métier, qui gère le côté fournisseurs et ne peut pas restaurer une sauvegarde.

CAPACITÉ	PROPRIÉTAIRE	ADMINISTRATEUR MÉTIER	ADMINISTRATEUR SYSTÈME	EXAMINATEUR	LECTEUR
Voit les fournisseurs et les documents	✓	✓	—	✓	✓
Ajoute et modifie des fournisseurs	✓	✓	—	—	—
Vérifie les documents et décide de l'approbation	✓	✓	—	✓	—
Voit les documents sensibles (données de paiement)	✓	✓	—	—	—
Gère les utilisateurs et les rôles	✓	✓	✓	—	—
Restaure une sauvegarde	✓	—	—	—	—

Des règles qu'aucun rôle ne peut contourner

- Personne — y compris le propriétaire — ne peut changer son propre rôle.
- Un administrateur ne peut ni créer ni rétrograder un compte avec le rôle propriétaire.
- Le dernier compte propriétaire ne peut être ni rétrogradé ni désactivé, afin que l'entreprise ne se retrouve jamais sans personne disposant des pleins pouvoirs.

- L'authentification à deux facteurs est obligatoire et impossible à ignorer pour le propriétaire, l'administrateur métier, l'administrateur système et le vérificateur. L'observateur peut l'activer, sans y être obligé.
- Une connexion échouée ne révèle jamais si c'est l'adresse ou le mot de passe qui est incorrect, donc l'écran ne peut pas servir à vérifier l'existence d'un compte.

Ce qui est stocké, qui peut y accéder, et pendant combien de temps.

Les documents sensibles exigent un droit distinct

Les documents fournisseurs ordinaires sont visibles par quiconque a accès à sa fiche. Les documents marqués sensibles — surtout liés au paiement — exigent un droit supplémentaire, réservé en pratique au propriétaire et à l'administrateur. Une tentative sans ce droit se solde par un refus, et ce refus est enregistré.

Les fichiers n'ont jamais d'adresse fixe

Le téléchargement passe par un lien signé numériquement, valable quelques minutes et lié à votre entreprise. L'ouvrir dans un autre contexte ne donne rien. Chaque téléchargement d'un fichier sensible est audité séparément.

Rétention : sept ans par défaut

Le réglage des documents et de la rétention est par défaut à 2555 jours, conforme aux exigences habituelles d'audit d'achats, et peut être modifié à tout moment. En toute honnêteté : il enregistre aujourd'hui votre politique et pilotera les futurs nettoyages — rien n'est supprimé automatiquement simplement parce qu'un délai est passé.

Les invitations expirent, et un renvoi les invalide

Le lien d'invitation est un jeton aléatoire à durée limitée, une semaine par défaut — volontairement pas à usage unique, pour que le fournisseur puisse revenir à un formulaire inachevé via le même lien. L'envoi d'une nouvelle invitation invalide immédiatement la précédente, même si elle a déjà été ouverte — c'est aujourd'hui le seul moyen de couper un lien ; il n'existe pas de bouton de révocation séparé.

Données bancaires chiffrées au repos

AES-256-GCM dès l'enregistrement. Le motif indiqué pour révéler le numéro va dans l'historique d'audit ; le numéro lui-même jamais.

Rapport support sans données

L'onglet diagnostic du centre système génère un rapport pour le support technique contenant versions, compteurs et lignes de journal masquées — jamais le contenu des documents, les données bancaires ni les données personnelles des fournisseurs.

Les questions qu'un auditeur pose en premier.

VendoCerta est-il un service cloud auquel nous confions nos données ?

Non. L'installation se fait sur une machine que vous contrôlez. PostgreSQL, le stockage de fichiers et l'aperçu de messagerie fonctionnent comme des binaires portables dans le dossier du projet — rien n'est installé au niveau de Windows, sans droits administrateur, Docker en option. Internet est nécessaire au premier démarrage pour télécharger ces services ; ensuite, l'installation vous appartient.

Recevons-nous une documentation technique au-delà de cette page ?

Oui. L'installation contient un modèle de sécurité et un modèle de menaces sous forme de documents dans le dépôt — les mêmes sources qui ont servi à cette page. Demandez-les à la personne qui gère votre installation, ou à nous via le formulaire de démonstration, en précisant que c'est pour une revue de sécurité.

À quoi l'assistant IA a-t-il accès ?

Uniquement à ce que la personne qui interroge peut déjà voir, et il n'exécute jamais une action sans sa confirmation explicite — les droits sont revérifiés au moment du clic, pour la personne qui clique. Il ne peut ni approuver, ni rejeter, ni suspendre un fournisseur, ni changer un rôle, ni rien supprimer.

La réinitialisation du mot de passe contourne-t-elle l'authentification à deux facteurs ?

Non. Pour les rôles où le second facteur est obligatoire, il l'est sur tout chemin vers le compte, y compris après une réinitialisation.

Où vont les e-mails pendant le pilote ?

Vers une boîte de prévisualisation locale sur l'installation elle-même, pas vers de vrais destinataires — pour que le pilote ne puisse pas écrire par erreur à un fournisseur. L'onglet installation du centre système indique quelle boîte une installation donnée utilise réellement.