AUTOQUOTE

Sécurité et résilience

Engagements et garanties techniques pour les autocaristes exigeants

Livre blanc · Édition 2026 · v1.0
Conforme RGPD · Accompagnement NIS2

Sommaire

CHAPITRE 01

Synthèse

Vos données protégées, votre exploitation tenue

Synthèse

À qui s'adresse ce livre blanc

Aux **dirigeants, DSI, RSSI et DPO des autocaristes** qui doivent comprendre, et justifier auprès de leurs donneurs d'ordres, le niveau de sécurité de la plateforme AutoQuote.

L'objectif n'est pas de raconter de la technique pour la technique. C'est de donner un **cadre d'engagement vérifiable** que vous pouvez joindre à un appel d'offres, présenter à un audit grand compte ou intégrer à votre registre des prestataires NIS2.

Ce que nous garantissons en une page

AutoQuote est la plateforme de gestion des devis pour les autocaristes. Nous traitons des données opérationnelles sensibles : portefeuilles de prospects, contrats, contenu commercial, plannings. Dans un secteur entrant dans le périmètre de la directive NIS2, **vos clients sont eux-mêmes des entités régulées** : et nous le savons.

Nos engagements sont conçus pour vous permettre de tenir les vôtres.

Confidentialité

- Hébergement exclusivement au sein de l'Union européenne
- Chiffrement par clé propre à AutoQuote, renouvelée régulièrement
- Coffre à secrets dédié, aucune donnée d'accès en clair
- Garde-fous structurels appliqués en amont des équipes

Disponibilité

- Réplication temps réel sur seconde région UE
- Retour à la normale en heures, perte maximale en minutes
- Restauration à la minute près sur une semaine glissante
- Adaptation automatique à vos pics d'activité

Intégrité

- Sauvegardes long terme verrouillées (anti-rançongiciel)
- Triple verrouillage technique des destructions
- Vérification cryptographique de chaque mise à jour

Traçabilité

- Journal d'audit immuable jusqu'à sept ans
- Supervision continue, une dizaine d'indicateurs critiques
- Engagement de notification d'incident sous vingt-quatre heures

Notre positionnement vis-à-vis de NIS2

AutoQuote n’est pas elle-même une entité régulée NIS2. Vos clients autocaristes le sont. Notre rôle est de leur fournir une infrastructure et des processus qui leur permettent de **tenir leurs propres obligations** : notamment la notification d’incident sous vingt-quatre heures, la traçabilité documentaire et la coopération en cas d’audit.

Comment lire ce livre blanc

Selon votre besoin du moment, trois parcours :

Vue d'ensemble · 10 min

- Cette synthèse (chap 1)
- Les 4 domaines (chap 3)
- Comment travailler (chap 7)

Audit fournisseur · 45 min

- Tout dans l'ordre
- Lecture lente du chap 4
- Plan incident (chap 6)

DPO · 30 min

- Synthèse (chap 1)
- Conformité (chap 5)
- Glossaire (annexe)

> *Nos engagements de sécurité ne sont pas du marketing. Ils sont implémentés en code, auditables, et contractuellement opposables.*

CHAPITRE 02

Le contexte

Pourquoi la sécurité est devenue un enjeu commercial pour l'autocariste

Le contexte

Le transport routier de voyageurs entre dans NIS2

La directive européenne NIS2 (Network and Information Security) a été transposée en droit français par la **loi du 30 juillet 2025**. Elle remplace NIS1 et étend considérablement son périmètre : la France passe d'environ 500 entités régulées à plusieurs milliers, dont une large partie des opérateurs de transport routier de voyageurs.

> **Les obligations qui retombent sur vous**
>
> Si votre entreprise est dans le champ de NIS2, vous devez notamment :
>
> - notifier l'ANSSI / CERT-FR sous **24 heures** en cas d'incident significatif ;
> - tenir un **inventaire des prestataires** qui traitent vos données opérationnelles ;
> - démontrer une **politique de sécurité documentée** couvrant vos sous-traitants ;
> - prouver votre **capacité de reprise** (RTO, RPO, tests de continuité) ;
> - répondre aux **audits** diligentés par les autorités.
>
> Les sanctions sont alignées RGPD : jusqu'à 2 % du chiffre d'affaires mondial pour les entités essentielles, 1,4 % pour les importantes.

Les donneurs d'ordres anticipent

Les grands donneurs d'ordres, collectivités, opérateurs nationaux, intercommunalités, n'attendent pas que vous soyez audités pour exiger des preuves. Les annexes sécurité des appels d'offres se sont durcies depuis 2024. Aujourd'hui, un autocariste qui ne peut pas fournir en moins d'une heure :

- son **registre des sous-traitants techniques**,
- son **avenant DPA** signé avec son prestataire SaaS,
- une **preuve de localisation européenne** des données,
- un **engagement de notification d'incident**,

… est mécaniquement disqualifié au tour suivant. Pas pour des raisons techniques, pour des raisons administratives.

Les rançongiciels frappent par les sous-traitants

Les attaques par rançongiciel ne ciblent plus seulement les grandes entreprises. Depuis 2023, les attaquants exploitent systématiquement la **chaîne des prestataires SaaS** : compromettre un fournisseur permet d'atteindre toutes ses PME clientes en une fois.

> *Les PME ne paient pas pour leur propre sécurité. Elles paient pour la sécurité du SaaS qu'elles utilisent.*

Pour une PME autocariste sans équipe sécurité dédiée, c'est **le niveau de sécurité de son SaaS** qui définit en pratique son niveau de sécurité global.

Ce que cela signifie pour AutoQuote

Pour vous, en tant qu'autocariste

- Conformité NIS2 facilitée
- Pièces prêtes pour appels d'offres
- Continuité de votre exploitation

Pour AutoQuote, vis-à-vis de vous

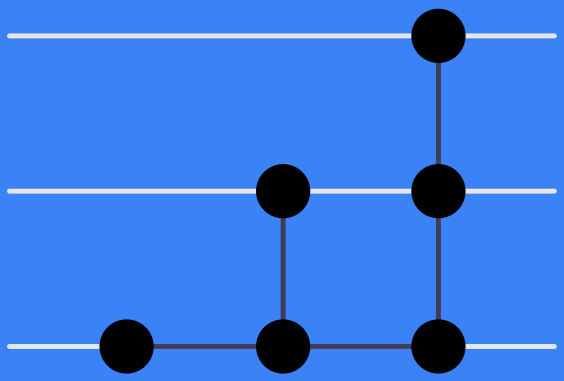
- Engagement contractuel de notification 24h
- Documentation tenue à jour
- Audit possible à tout moment

Pour AutoQuote, en interne

- Architecture refondue en 2026
- Validation par un grand opérateur transport
- Investissement structurel continu

Refonte d'architecture 2026

AutoQuote a été refondue en 2026 pour répondre aux exigences d'audit d'un acteur majeur du transport routier de voyageurs. La plateforme actuelle est le résultat de cette mise à niveau : **les 12 garanties techniques décrites dans le chapitre 4 sont la conséquence directe de cet audit**. Ce que vous lisez n'est pas une déclaration d'intention. C'est ce qui est implémenté, en production, et auditable.



CHAPITRE 03

Les 4 domaines

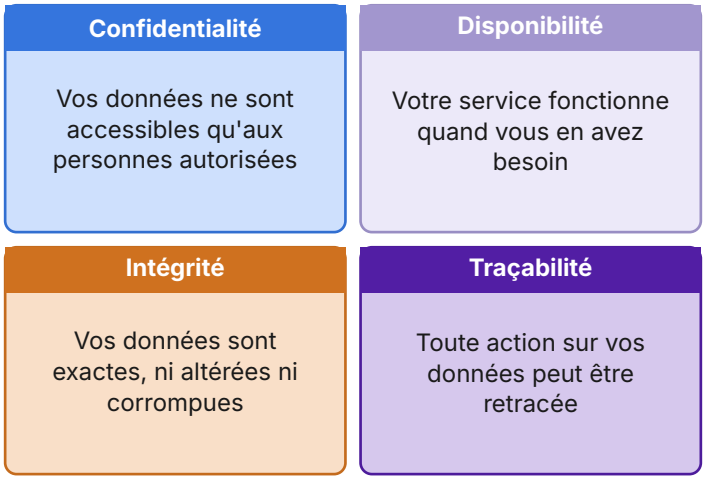
La grille de lecture d'un audit grand compte

Les 4 domaines de garantie

Une grille de lecture universelle

Tous les référentiels d'audit sérieux, ISO 27001, NIS2, RGPD article 32, CIS Controls, EBIOS, structurent la sécurité d'un système autour de quatre propriétés fondamentales.

> **Les quatre propriétés que doit tenir un SaaS**
>
> 1. **Confidentialité** : vos données ne sont accessibles qu'aux personnes autorisées.
> 2. **Disponibilité** : votre service fonctionne quand vous en avez besoin.
> 3. **Intégrité** : vos données sont exactes, n'ont pas été altérées par erreur ou malveillance.
> 4. **Traçabilité** : toute action sur vos données peut être retracée et auditée.



AutoQuote structure ses engagements selon cette grille. Cela permet à votre DSI, DPO ou auditeur externe de mapper rapidement nos garanties à son propre référentiel, sans devoir réinventer la roue.

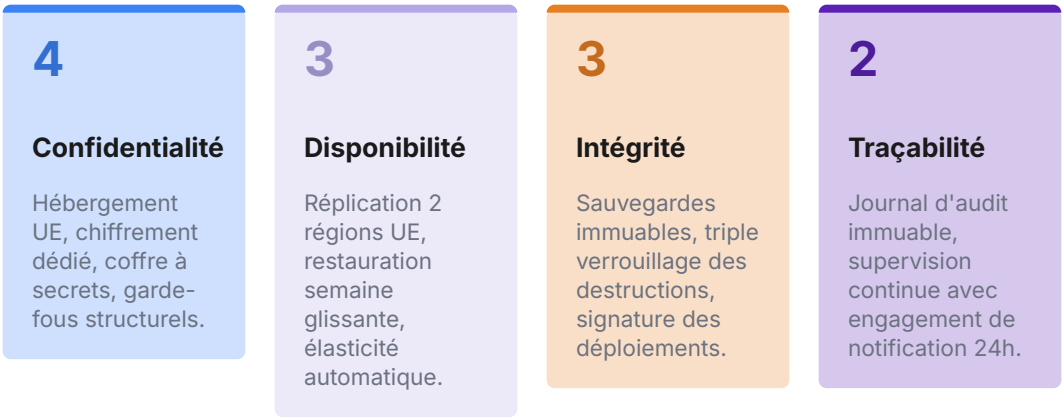
Pourquoi cette grille importe pour vous

Propriété	Ce que vous perdez si elle tombe	Conséquence opérationnelle
Confidentialité	Une fuite expose votre portefeuille client	Avantage concurrentiel perdu, déclaration CNIL, perte de confiance

Disponibilité	Le service est inaccessible un vendredi 17h	Devis non envoyés, opportunités commerciales manquées
Intégrité	Un import écrase 50 contacts existants	Données reconstituées à la main, perte de productivité
Traçabilité	Vous ne pouvez pas démontrer qui a fait quoi	Impossible de répondre à un audit grand compte

Comment AutoQuote couvre les quatre

Le chapitre 4 détaille les **12 garanties techniques** organisées par domaine :



Comment lire le chapitre suivant

Chaque garantie est présentée avec :

- **Ce que nous promettons** : l'engagement formel ;
- **Ce que cela évite** : la situation opérationnelle évitée ;
- **Comment c'est implémenté** : le principe technique, sans détails opérationnels sensibles.

Les détails opérationnels précis (noms de composants, paramétrages, configurations) sont fournis sur demande aux clients sous contrat, dans le cadre d'un engagement de confidentialité. Nous ne publions pas ces informations en accès libre, par bonne hygiène de sécurité.

> *Un livre blanc qui détaille trop son architecture aide les attaquants. Un livre blanc qui ne dit rien n'aide personne. Nous avons cherché le juste équilibre.*

CHAPITRE 04

Les 12 garanties

Le cœur opérationnel de nos engagements

Les 12 garanties techniques

Confidentialité (4 garanties)

Garantie 1 : Hébergement 100 % souverain UE

Ce que nous promettons : Vos données sont stockées exclusivement au sein de l'Union européenne, sur deux régions distinctes. Elles ne sortent jamais de ce périmètre dans le cadre nominal du Service. Cet engagement est inscrit au contrat et opposable à AutoQuote.

Ce que cela évite : L'application du CLOUD Act américain ou de toute juridiction extra-européenne sur vos données opérationnelles. La perte de souveraineté lors d'un changement de fournisseur cloud côté prestataire.

Comment c'est implémenté : Sélection de régions cloud certifiées au sein de l'Union européenne. Architecture déployée intégralement dans ce périmètre, sans dépendance technique vers une région hors UE.

Garantie 2 : Chiffrement par clé propre AutoQuote

Ce que nous promettons : Toutes vos données stockées sont chiffrées au repos par une clé cryptographique dédiée à AutoQuote, **distincte** de toute clé partagée par défaut du fournisseur cloud. Cette clé est renouvelée automatiquement et régulièrement.

Ce que cela évite : Le risque qu'une faille générique sur les clés partagées du fournisseur ne mette en cause vos données. La perte de contrôle sur la rotation et la traçabilité du chiffrement.

Comment c'est implémenté : Stratégie de clés gérées par le client (modèle CMEK), gestion via un service de gestion de clés cryptographique certifié.

Rotation automatique régulière, délai de destruction différé pour éviter les suppressions accidentelles.

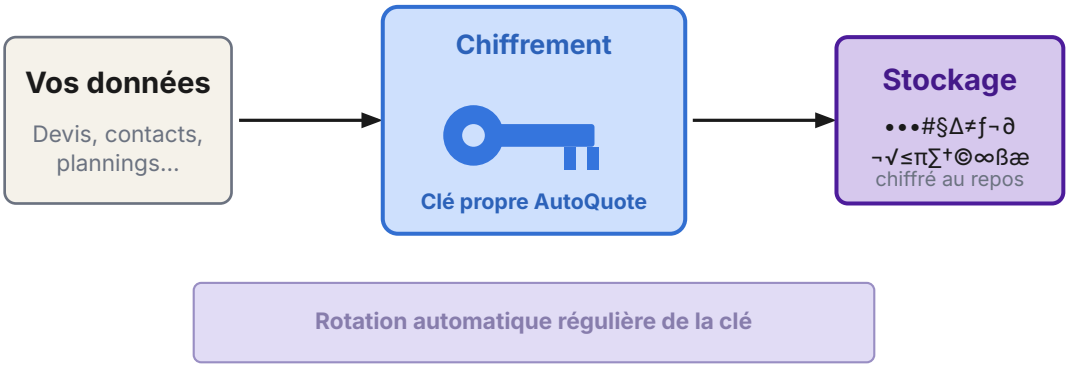


Figure : Aucune donnée n'arrive en clair dans le stockage : elle traverse systématiquement notre clé dédiée, renouvelée chaque trimestre.

Garantie 3 : Coffre à secrets

Ce que nous promettons : Tous les identifiants techniques (mots de passe applicatifs, clés d'API, jetons d'accès) sont stockés dans un coffre dédié. **Aucun secret n'est en clair** dans le code applicatif, les configurations ou les pipelines. L'accès au coffre est journalisé.

Ce que cela évite : La compromission massive d'accès via une fuite de code source. La présence de secrets oubliés dans des sauvegardes Git ou des historiques de configuration.

Comment c'est implémenté : Coffre à secrets managé, intégration native avec les composants applicatifs. Rotation périodique adaptée à la sensibilité de chaque secret.

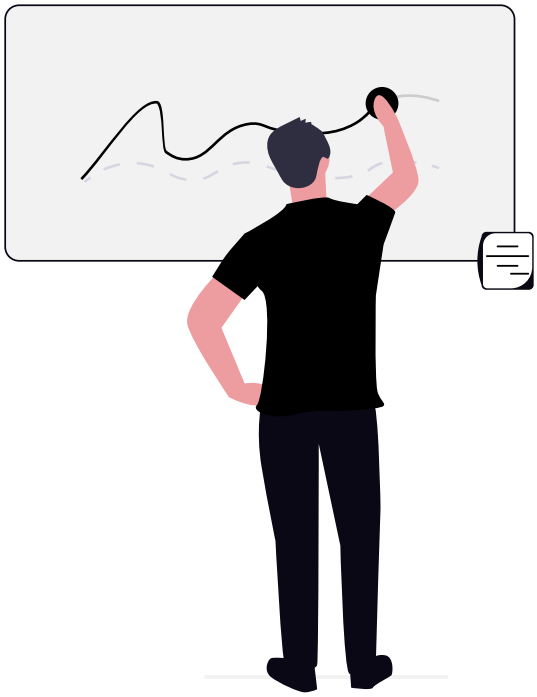
Garantie 4 : Garde-fous structurels appliqués en amont

Ce que nous promettons : Une **quinzaine de règles techniques bloquantes** encadrent l'activité quotidienne des équipes et des pipelines. Elles définissent ce qu'il est possible de faire ou non, indépendamment du collaborateur qui agit. Un développeur isolé ne peut pas les contourner.

Ce que cela évite : Les erreurs opérationnelles dues à un membre d'équipe distrait, fatigué, ou, dans le pire des cas, compromis. L'écart entre la politique théorique et la pratique réelle.

Comment c'est implémenté : Politiques de refus IAM, filtrage applicatif des requêtes (OWASP Core Rule Set), restriction géographique des accès, limitation de débit par route, vérification cryptographique des déploiements.

Disponibilité (3 garanties)



Garantie 5 : Réplication temps réel sur 2 régions UE

Ce que nous promettons : Vos données sont copiées en continu sur deux régions géographiques séparées en Europe. Si la région principale tombe, nous basculons sur la seconde.

Ce que cela évite : Une indisponibilité prolongée en cas de panne majeure sur une région cloud (incident électrique, panne réseau, sinistre).

Comment c'est implémenté : Instance répliquée en seconde région européenne, en mode réplication continue. Bascule documentée et exercée.

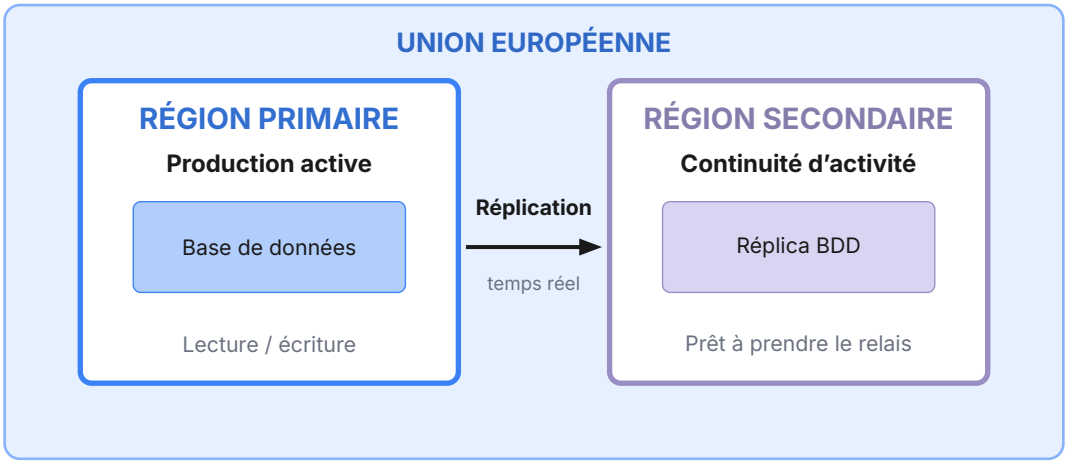


Figure : Architecture multi-régions au sein de l'Union européenne : votre base de données est répliquée en continu sur deux régions distinctes.

Vos objectifs de reprise

- **RTO** (temps de retour à la normale) : **quelques heures**
- **RPO** (perte de données maximale) : **quelques minutes**

Garantie 6 : Restauration sur une semaine glissante

Ce que nous promettons : Vous pouvez restaurer vos données à n'importe quel instant de la **semaine écoulée**, **à la minute près**. Une demande de restauration urgente est traitée en quelques heures.

Ce que cela évite : La perte définitive de données en cas d'erreur humaine, d'import mal paramétré, ou de corruption logique d'une intégration tierce.

Comment c'est implémenté : Conservation continue des journaux de transactions de la base de données, permettant la restauration à n'importe quel instant de la fenêtre de rétention.

Figure : Sur la fenêtre des 7 derniers jours, vous pouvez restaurer votre base à n'importe quel instant, pas seulement aux sauvegardes quotidiennes.

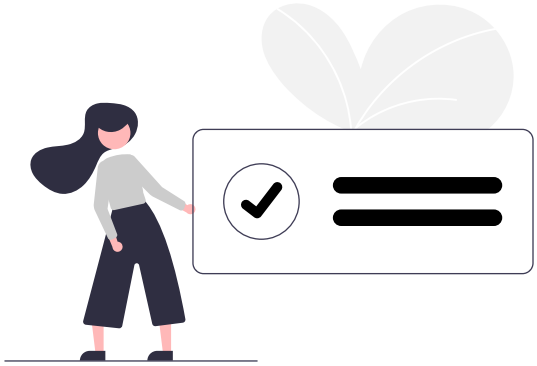
Garantie 7 : Élasticité automatique

Ce que nous promettons : La capacité de calcul de la plateforme s'ajuste automatiquement à votre activité. Aucune intervention manuelle lors des pics commerciaux (rentrée scolaire, périodes de forte demande, gros appels d'offres simultanés).

Ce que cela évite : La dégradation de service au pire moment, typiquement quand votre exploitation a le plus besoin de la plateforme.

Comment c'est implémenté : Composant applicatif en mode serverless avec autoscaling natif sur les métriques de charge.

Intégrité (3 garanties)



Garantie 8 : Sauvegardes long terme immuables

Ce que nous promettons : Les archives long terme sont déposées dans un coffre numérique **verrouillé par une politique de rétention non modifiable**. Une fois déposée, une archive ne peut être altérée ou supprimée avant son échéance, y compris par un administrateur d'AutoQuote. Parade efficace contre les attaques par rançongiciel ciblant les sauvegardes.

Ce que cela évite : Le scénario typique d'un rançongiciel qui chiffre les données **et** leurs sauvegardes, rendant impossible toute restauration sans paiement.

Comment c'est implémenté : Espaces de stockage avec verrouillage de rétention activé (le contenu ne peut être ni modifié ni supprimé avant l'échéance). Durées de rétention adaptées : jusqu'à 7 ans pour les journaux d'administration, 1 an pour les journaux d'accès, 90 jours pour les configurations.

Trois niveaux de rétention selon la sensibilité

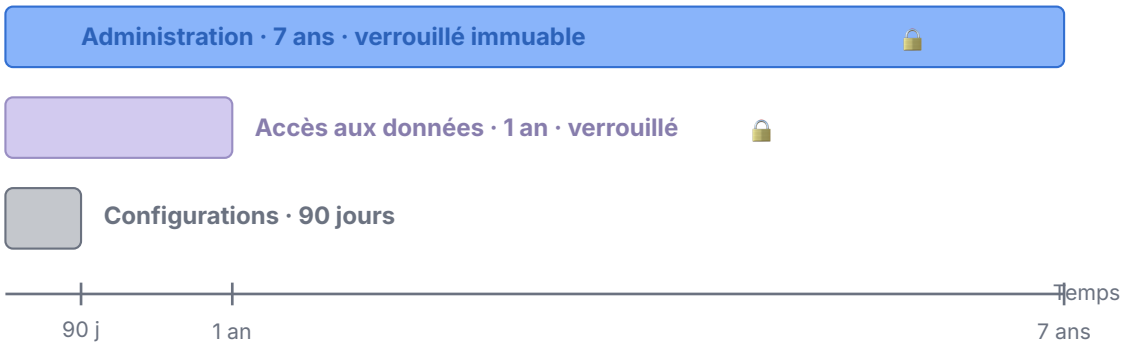


Figure : Les journaux d'administration sont verrouillés sept ans dans un coffre immuable. Aucun administrateur AutoQuote ne peut les altérer avant l'échéance.

Garantie 9 : Triple verrouillage des destructions

Ce que nous promettons : Plusieurs mécanismes techniques **indépendants et complémentaires** bloquent les suppressions sensibles. Aucune erreur isolée, ni même un compte compromis, ne peut casser votre instance.

Ce que cela évite : La suppression accidentelle ou malveillante de votre base de données ou de votre stockage. Le « click de trop » destructeur.

Comment c'est implémenté : Protection au niveau de la ressource (drapeau de protection à la suppression), au niveau du code d'infrastructure (refus en amont), et au niveau des autorisations (les pipelines automatisés sont privés du droit de supprimer).

Garantie 10 : Vérification cryptographique des mises à jour

Ce que nous promettons : Chaque nouvelle version applicative est **signée cryptographiquement** avant publication. Notre infrastructure refuse automatiquement toute version dont la signature ne correspond pas.

Ce que cela évite : L'injection d'une version malveillante via une attaque sur notre chaîne de fabrication logicielle (typique des attaques de supply chain).

Comment c'est implémenté : Politique de signature et de vérification automatique des images applicatives à l'exécution. Toute image non signée par notre chaîne officielle est bloquée à la porte du runtime.

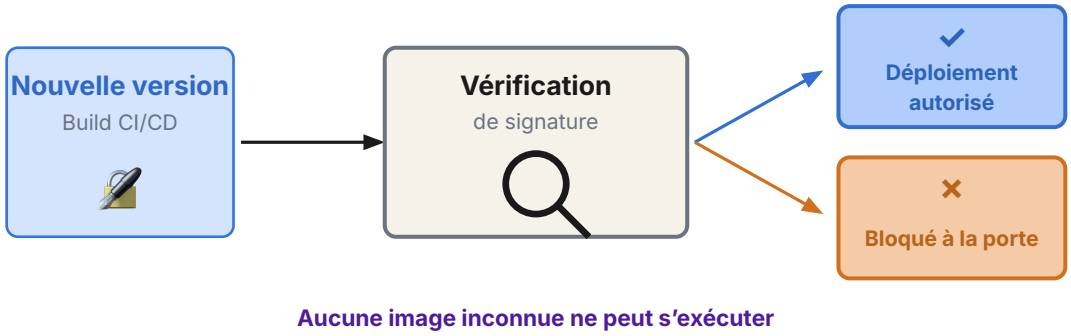
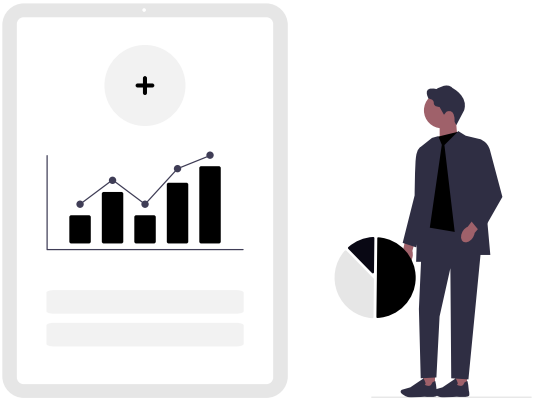


Figure : Chaque version applicative est signée puis vérifiée avant exécution. Une image injectée par une attaque sur la chaîne de fabrication est rejetée à la porte du runtime.

Traçabilité (2 garanties)



Garantie 11 : Journal d'audit immuable

Ce que nous promettons : Toute action sensible sur la plateforme est **enregistrée et conservée**. Les journaux sont stockés dans le coffre immuable décrit en garantie 8. Exploitables en cas de contrôle externe ou d'enquête interne.

Ce que cela évite : L'incapacité à démontrer qui a fait quoi en cas d'audit, d'incident ou de litige.

Comment c'est implémenté : Activation des journaux d'audit administration sur l'ensemble des composants. Export vers le coffre verrouillé avec rétention jusqu'à **sept ans** pour les journaux d'administration. Les journaux d'accès aux données sensibles font l'objet d'une conservation distincte sur un an.

Garantie 12 : Supervision 24/7 avec plan d'incident

Ce que nous promettons : Une dizaine d'**indicateurs critiques** sont surveillés en continu par un système d'alerte automatisé. Équipe d'astreinte mobilisable. **Engagement contractuel de notification d'incident sous 24 heures** pour vous permettre, si vous êtes soumis à NIS2, de tenir vos propres obligations.

Ce que cela évite : Un incident significatif chez nous qui resterait silencieux et compromettrait vos propres déclarations CERT-FR.

Comment c'est implémenté : Système de monitoring avec règles d'alerte sur dégradation de disponibilité, intégrité des sauvegardes, dérive de configuration de sécurité, comportement anormal de coût. Procédure d'astreinte documentée. Plan de réponse à incident détaillé au chapitre 6.

> *Douze garanties techniques, quatre domaines, un seul objectif : que vous puissiez répondre « oui » à tout questionnaire de sécurité, contrat à l'appui.*

CHAPITRE 05

Conformité

RGPD, NIS2 et accompagnement de vos obligations

Conformité

Notre positionnement

> **Ce que nous sommes, et ce que nous ne sommes pas**
>
> - **AutoQuote est sous-traitant** au sens de l'article 28 du RGPD pour les données que vous nous confiez.
> - **AutoQuote n'est pas une entité régulée NIS2** en tant que telle. Vos clients autocaristes, eux, peuvent l'être.
> - Notre rôle est de vous **aider à tenir vos obligations**, sans prétendre nous-mêmes à un statut que nous n'avons pas.

Notre dispositif RGPD

Avenant de sous-traitance (DPA)

Nous mettons à disposition un **avenant de sous-traitance des données** (DPA) standard, conforme à l'article 28 du RGPD. Il :

- décrit la **nature et la finalité** des traitements ;
- liste les **catégories de données** et de personnes concernées ;
- fixe les **durées de conservation** ;
- formalise nos **obligations de sécurité** (ce livre blanc en annexe) ;
- prévoit la **notification de violation sous 24 heures** ;
- définit les **modalités d'audit** et de fin de relation.

Le DPA est fourni **sur demande** aux prospects qualifiés et clients sous contrat. Il est annexé à votre registre des traitements.

Sous-traitants techniques

La liste nominative de nos sous-traitants techniques, avec finalité, données traitées, localisation et base de transfert le cas échéant, est **fournie aux clients sous contrat**. Les changements font l'objet d'une **notification préalable**, conformément à l'article 28.2 du RGPD.

Pour anticiper votre lecture, les sous-traitants relèvent des catégories suivantes :

Catégorie	Finalité
Hébergement cloud	Infrastructure applicative et base de données
Intelligence artificielle	Assistance à la rédaction et analyse documentaire
Cartographie	Calcul d'itinéraires autocar spécialisés
Messagerie transactionnelle	Envoi d'emails de devis et notifications
Supervision applicative	Détection des erreurs techniques

CRM et support	Gestion de la relation et messagerie support
Mesure d'audience	Statistiques de fréquentation du site marketing

Tout transfert éventuel hors UE est encadré par les **Clauses Contractuelles Types** (CCT) de la Commission européenne (décision d'exécution 2021/914).

Droits des personnes concernées

AutoQuote met à disposition les outils techniques nécessaires pour répondre aux demandes d'exercice des droits (accès, rectification, effacement, portabilité, opposition, limitation). Le Client demeure responsable de la réponse aux personnes concernées ; nous fournissons les éléments techniques utiles.

> **Contact RGPD AutoQuote** : `contact@autoquote.tech`. Réponse sous trois jours ouvrés en moyenne.

Notre accompagnement NIS2

Le périmètre de la directive

La directive NIS2 (Network and Information Security 2) a été transposée en France par la **loi du 30 juillet 2025**. Elle s'applique aux **entités essentielles** (EE) et **entités importantes** (EI) dans 18 secteurs critiques, dont le **transport routier de voyageurs** au-delà de certains seuils de taille.

Critère	Entité essentielle	Entité importante
Seuil employés	≥ 250	≥ 50
Seuil CA	> 50 M€ ou bilan > 43 M€	> 10 M€ ou bilan > 10 M€
Délai notification incident	24 heures	24 heures
Sanction maximale	10 M€ ou 2 % CA mondial	7 M€ ou 1,4 % CA mondial

Ce que nous nous engageons à faire pour vous

Si vous êtes dans le périmètre NIS2, vous devez démontrer que vos prestataires techniques permettent votre conformité. AutoQuote s'engage à :

01

Notification sous 24h

Engagement contractuel de notification de tout incident significatif sous 24 heures, avec un dossier d'information utilisable pour votre propre déclaration CERT-FR.

02

Documentation utile

Mise à disposition de la documentation utile à votre registre des prestataires, votre annexe sécurité et vos audits internes.

03

Coopération aux audits

Réponse aux audits diligentés par vos soins ou par un tiers que vous mandatez, dans les conditions prévues par l'avenant DPA.

04

Préavis aux changements

Notification préalable de tout changement structurel impactant la sécurité (sous-traitants, architecture, conditions contractuelles).

Audits

Tout client peut demander, dans les conditions prévues par l’avenant DPA, un audit de nos engagements :

- **Mise à disposition de la documentation** technique détaillée sous accord de confidentialité ;
- **Présentation en visioconférence** des mécanismes en place, ouverte aux DSI, RSSI et DPO clients ;
- **Audit indépendant** par un tiers mandaté, sur préavis raisonnable, dans les conditions de l’article 28 du RGPD.

> *Le bon sous-traitant n'est pas celui qui revendique le plus. C'est celui qui rend votre conformité plus simple, pas plus difficile.*

CHAPITRE 06

Plan d'incident

Comment nous réagissons quand quelque chose ne va pas

Plan de réponse aux incidents

Pourquoi un plan documenté

Aucune plateforme n'est invulnérable. Ce qui distingue un prestataire sérieux d'un prestataire improvisé, c'est la **qualité de sa réponse quand l'incident survient**.

Un plan documenté permet :

- une **réaction coordonnée** sous pression ;
- une **qualification rapide** de la sévérité ;
- une **notification fiable** à nos clients dans les délais ;
- un **retour d'expérience** qui durcit le système pour la fois suivante.

Notre classification de sévérité

Tout événement est qualifié selon une échelle de quatre niveaux. Les niveaux S1 et S2 sont des **incidents significatifs** : ceux qui déclenchent l'engagement de notification sous 24 heures.

S1 Critique	S2 Élevée	S3 Modérée	S4 Mineure
Données compromises ou indisponibilité totale	Attaque ou indispo partielle	Vulnérabilité non exploitable	Anomalie sans impact
Notification immédiate	Notification < 24 h	Rapport mensuel	Traitement opérationnel

Les sept phases de la réponse

Notre procédure suit sept phases, de la détection à l'apprentissage. La notification client (phase 4) intervient sous 24 heures pour tout incident significatif.

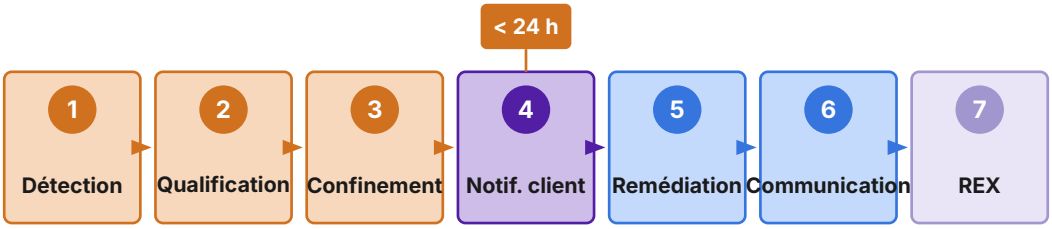


Figure : Les sept phases de notre plan de réponse. L'engagement contractuel de notification sous 24 heures intervient en phase 4.

1. **Détection** : par alerte automatisée, signalement client ou tiers de confiance.
2. **Qualification** : diagnostic initial, détermination de la sévérité et du périmètre touché.
3. **Confinement** : isolation, rotation des accès compromis, bascule régionale si nécessaire.
4. **Notification client** : sous 24 h pour S1/S2, par email aux contacts désignés au contrat.
5. **Remédiation** : correctifs logiciels ou de configuration, selon la sévérité.
6. **Communication** : mises à jour régulières jusqu'à clôture, rapport de clôture sous 14 jours.
7. **Retour d'expérience** : analyse de cause racine, mesures préventives, mise à jour de la documentation.

+ **Apprentissage** : le système est durci pour que l'incident ne puisse pas se reproduire.

Cas spécifiques anticipés

Attaque par rançongiciel

L'architecture de **sauvegardes long terme immuables** (garantie 8) constitue la parade structurelle. Aucun administrateur AutoQuote ne peut altérer les sauvegardes avant leur échéance de rétention.

La procédure prévoit le confinement du périmètre touché, l'évaluation de l'intégrité des sauvegardes verrouillées, et la restauration sur infrastructure propre depuis la dernière sauvegarde antérieure à la compromission.

> **AutoQuote ne paye pas de rançon.** Ce n'est pas une posture morale, c'est une décision opérationnelle : payer crée une asymétrie qui finance les attaques suivantes contre d'autres acteurs du secteur.

Demande d'autorité

Toute demande d'autorité (CNIL, autorité judiciaire) portant sur des données du Client est traitée par notre référent juridique. Le Client est notifié **sauf interdiction légale formelle** (typiquement, secret d'enquête).

Indisponibilité régionale prolongée

Au-delà d'un seuil de criticité, bascule sur la région de continuité européenne. Communication client toutes les 2 heures pendant la bascule. Retour à la région primaire après stabilisation et tests d'intégrité.

Tests et exercices

Le plan de réponse fait l'objet de tests réguliers :

Type de test	Fréquence

Restauration de sauvegarde sur environnement de recette	Trimestrielle
Test de bascule régionale avec mesure du RTO réel	Semestrielle
Exercice de simulation d’incident (scénario tiré au sort)	Annuelle
Revue du plan avec intégration des enseignements	Annuelle

Les résultats peuvent être présentés sur demande.

Pour signaler un incident

Si vous constatez un comportement suspect sur AutoQuote, contactez :

> **Signalement et coordination** : `contact@autoquote.tech`
> En cas d’urgence pendant un incident en cours : canal opérationnel défini avec votre interlocuteur commercial.

CHAPITRE 07

Travailler ensemble

Comment obtenir les documents et les preuves dont vous avez besoin

Travailler avec AutoQuote

Notre philosophie de transparence

> **Trois principes qui guident notre communication**
>
> 1. **Engagements vérifiables** : chaque garantie technique est implémentée en code, auditable. Pas du marketing, du contractuel.
> 2. **Confidentialité maîtrisée** : les détails opérationnels précis et la liste de nos sous-traitants sont communiqués sous engagement de confidentialité. Pas en accès libre.
> 3. **Accompagnement client** : nous fournissons à nos clients régulés les engagements et la documentation utiles à leurs propres obligations, plutôt que de leur compliquer la tâche.

Les documents disponibles

En accès libre

Vous pouvez télécharger librement sur `autoquote.tech` :

- **Ce livre blanc sécurité** : engagements, garanties et architecture.
- **La page produit sécurité et résilience** : vue d'ensemble, cas d'usage, FAQ.
- **Le statut du service en temps réel** : disponibilité mesurée en continu.
- **Les mentions légales** : identité juridique, hébergeur, droits sur les données.

Sur demande aux prospects qualifiés

Si vous évaluez sérieusement AutoQuote et que vous avez besoin de pièces formelles pour votre processus interne :

Document	Pour quoi faire	Modalité
Avenant DPA RGPD	Annexe juridique à votre contrat	Email simple
Présentation technique	Démo en visioconférence pour votre DSI/RSSI	Visio + NDA

Sur demande aux clients sous contrat

Une fois la relation contractuelle établie :

Document	Pour quoi faire	Modalité
Liste détaillée des sous-traitants	Registre RGPD article 28 et notifications	Email + NDA
Plan de réponse incident détaillé	Documentation de votre dispositif NIS2	Email + NDA

Présentation d'architecture	Audit interne, certification	Visio + NDA
Audit indépendant par tiers mandaté	Conformité grand compte	Préavis 30 j + NDA

Comment formuler votre demande

Email type à `contact@autoquote.tech`

Objet : Demande de [DPA / liste sous-traitants / plan incident / présentation architecture]

Corps :

- Votre nom et votre fonction ;
- Votre entreprise et votre statut vis-à-vis de NIS2 (entité essentielle, importante, hors scope) ;
- Le projet ou contexte de la demande (appel d'offres, audit, renouvellement contrat, etc.) ;
- La date à laquelle vous souhaitez recevoir le document.

Réponse sous **trois jours ouvrés** en moyenne.

Engagement de relation

Notification des changements

Tout changement structurel impactant la sécurité, nouveau sous-traitant accédant à des données personnelles, modification de localisation des données, changement de procédure de notification, fait l'objet d'une **notification préalable par email** aux contacts RGPD que vous nous avez désignés.

Vous disposez d'un délai raisonnable pour formuler d'éventuelles objections motivées.

Revue annuelle

Tout client sous contrat peut demander une **revue annuelle** en visioconférence avec notre équipe sécurité : évolutions de l'architecture, retours d'expérience de l'année écoulée, mises à jour de la documentation, anticipation des évolutions réglementaires.

> *Un bon prestataire technique n'est pas celui qui dit non aux questions. C'est celui qui structure les réponses pour qu'elles soient utiles à votre DPO.*

Démarrer

Si vous découvrez AutoQuote et que vous voulez creuser la dimension sécurité avant d'aller plus loin :

1

Une démo produit

Pour comprendre comment AutoQuote s'intègre dans votre exploitation.

2

Une session sécurité

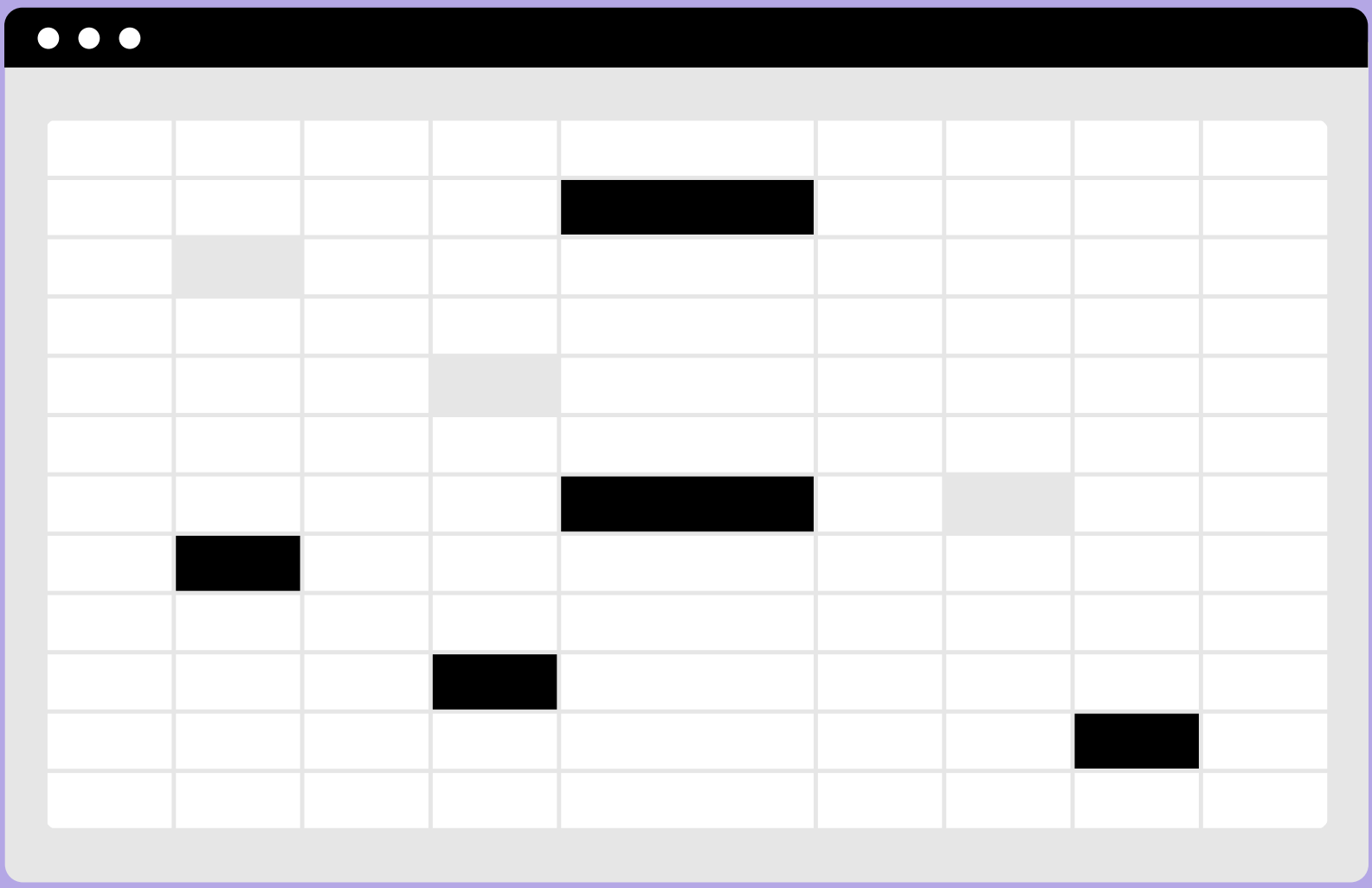
Pour votre DSI/RSSI/DPO, en visio, 45 minutes, sans engagement.

3

Un POC contrôlé

Sur un périmètre limité, avec DPA signé, pour valider en conditions réelles.

Tous les chemins commencent ici : `contact@autoquote.tech` ou via le formulaire sur `autoquote.tech/contact`.



CHAPITRE 08

Glossaire

Le vocabulaire sécurité utile pour comprendre ce livre blanc

Glossaire

Vocabulaire utile

Les termes que vous croiserez dans ce livre blanc, dans nos contrats, ou dans une discussion avec un DPO.

Terme	Définition
CCT	Clauses Contractuelles Types, modèle juridique standard de la Commission européenne pour encadrer un transfert de données hors UE (décision 2021/914).
CERT-FR	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. Service de l'ANSSI. Autorité de notification d'incident pour les entités NIS2.
Chiffrement au repos	Le chiffrement des données pendant qu'elles sont stockées (par opposition au chiffrement en transit, qui les protège quand elles circulent sur le réseau).
CMEK	Customer-Managed Encryption Key, modèle où le client de la solution cloud (en l'occurrence AutoQuote) gère sa propre clé cryptographique, distincte des clés partagées par défaut du fournisseur.
CNIL	Commission Nationale de l'Informatique et des Libertés, autorité française de protection des données personnelles, compétente pour le RGPD.
DPA	Data Processing Agreement, avenant de sous-traitance des données. Document contractuel qui formalise les engagements RGPD entre responsable de traitement et sous-traitant.
DPO	Data Protection Officer, délégué à la protection des données. Personne responsable du dispositif RGPD au sein d'une organisation.
EBIOS	Méthode française d'analyse de risque cyber maintenue par l'ANSSI. Référentiel courant pour les RSSI et auditeurs sécurité.
Entité essentielle (EE)	Catégorie haute de la directive NIS2. Concerne les organisations critiques de grande taille dans 11 secteurs prioritaires.
Entité importante (EI)	Catégorie basse de la directive NIS2. Couvre des secteurs additionnels avec des seuils plus bas, dont le transport routier de voyageurs.
IAM	Identity and Access Management, gestion des identités et des autorisations sur une plateforme cloud.

NIS2	Network and Information Security 2, directive européenne 2022/2555 sur la cybersécurité. Transposée en France par la loi du 30 juillet 2025.
OWASP CRS	OWASP Core Rule Set, ensemble de règles de filtrage applicatif standard, maintenu par la fondation OWASP, qui bloque les attaques web courantes (injection, cross-site scripting…).
PITR	Point-In-Time Recovery, capacité technique de restaurer une base de données à un instant précis du passé, sans avoir à reposer sur une sauvegarde quotidienne grossière.
Rançongiciel	Logiciel malveillant qui chiffre les données d'une organisation et exige une rançon pour les déchiffrer. Cible désormais systématiquement les sauvegardes.
RGPD	Règlement Général sur la Protection des Données, règlement (UE) 2016/679. Cadre européen de protection des données personnelles, applicable depuis mai 2018.
RPO	Recovery Point Objective, perte de données maximale admissible exprimée en temps. RPO = 5 min signifie qu'on accepte au pire de perdre 5 minutes de données récentes.
RSSI	Responsable de la Sécurité des Systèmes d'Information. Fonction sécurité au sein d'une DSI.
RTO	Recovery Time Objective, temps de reprise maximal admissible exprimé en temps. RTO = 2 h signifie que le service doit redevenir disponible en moins de 2 heures.
Secret Manager	Coffre à secrets managé par un fournisseur cloud, qui stocke et chiffre les identifiants techniques, journalise les accès et permet la rotation périodique.
Sous-traitant	Au sens du RGPD article 28 : tiers technique qui traite des données personnelles pour le compte du responsable de traitement. En l'occurrence, AutoQuote est sous-traitant pour ses clients.
Sous-traitant ultérieur	Sous-traitant du sous-traitant. Au sens du RGPD, AutoQuote doit déclarer ses propres sous-traitants ultérieurs à ses clients (article 28.2).
Supply chain (attaque de)	Attaque qui compromet un maillon de la chaîne de fabrication logicielle (dépendance, image conteneur, pipeline) plutôt que la cible finale directement.
TLS	Transport Layer Security, protocole standard de chiffrement des communications réseau. Successeur de SSL.
Verrouillage de rétention	Mécanisme technique (parfois appelé *Object Lock*) qui verrouille un espace de stockage en empêchant toute modification ou suppression jusqu'à la fin d'une période fixée. Aucun

	administrateur, aucun script ne peut contourner. Parade structurelle au rançongiciel.
WAF	Web Application Firewall, pare-feu applicatif qui filtre les requêtes HTTP malveillantes avant qu'elles n'atteignent l'application.
Workload Identity	Mécanisme moderne qui permet à un pipeline d'authentifier sans clé statique de longue durée. Réduit drastiquement le risque de fuite d'identifiants.

Pour aller plus loin

Référentiels officiels

- Texte NIS2, eur-lex.europa.eu
- Loi française du 30 juillet 2025
- RGPD, gdpr-info.eu
- EBIOS Risk Manager, ANSSI

Ressources pratiques

- CNIL, cnil.fr (RGPD)
- CERT-FR, cert.ssi.gouv.fr (NIS2)
- ANSSI, ssi.gouv.fr (cyber)
- OWASP Top 10, owasp.org

Une question sur un terme non listé ? Notre équipe RGPD répond à `contact@autoquote.tech`.

AUTOQUOTE

PROTECT

Protéger vos données, tenir votre exploitation.

Scannez pour
nous contacter

Discutons de votre projet · autoquote.tech

Livre blanc sécurité · édition 2026 · v1.0 · Conforme RGPD · Accompagnement NIS2 · Illustrations Undraw (MIT) + Open Doodles (CC0)