VisionLink

Audit de conformité RGPD

Date du rapport : 11/05/2026

Plateforme de support à distance par caméra avec IA

Domaine audité : vlink.space

Édité et commercialisé par : Techmaverick Ltd

1. Résumé exécutif

VisionLink est une plateforme SaaS qui permet à un client de partager sa caméra de smartphone avec un technicien à distance, avec assistance IA optionnelle et contrôle à distance du PC. Cet audit vérifie la conformité au **Règlement (UE) 2016/679 (RGPD)** et identifie les mesures techniques et organisationnelles en place pour protéger les données personnelles.

Verdict global : Conforme RGPD.

Responsable du traitement

Techmaverick Ltd — éditeur et exploitant commercial de la plateforme VisionLink (vlink.space). Contact RGPD : **contact@vlink.space**.

État de conformité par domaine clé

Domaine	État	Commentaire
Bases légales du traitement	✓ OK	Consentement + intérêt légitime
Hébergement données (UE)	✓ OK	Hostinger France + SMTP client + SMS.to UE
Chiffrement en transit	✓ OK	HTTPS/TLS + DTLS/SRTP (WebRTC)
Chiffrement au repos	✓ OK	BDD + S3 chiffrés au repos
Droits des personnes	✓ OK	Accès / suppression via support
Durée de conservation	✓ OK	Streams non enregistrés par défaut
Sécurité (TLS, HSTS, RL)	✓ OK	HSTS, rate limiting, bcrypt
Sous-traitants (Art. 28)	✓ OK	Liste publiée dans la politique de confidentialité
Registre des traitements	✓ OK	Document interne formalisé (Art. 30)
Contact RGPD	✓ OK	contact@vlink.space

2. Infrastructure et localisation des données

Toutes les données traitées par VisionLink transitent et sont stockées exclusivement au sein de l'Union européenne (UE) ou via des sous-traitants présentant des garanties équivalentes (Clauses Contractuelles Types).

Cartographie des composants

Composant	Fournisseur / Localisation	Type de données
Serveur TURN/STUN (WebRTC relay)	Hostinger VPS — France ■■	Flux vidéo chiffré DTLS/SRTP (relais uniquement)
Serveur TURN backup	Xirsys (UE) + ExpressTurn (UE)	Idem, relais uniquement
Application web	Hébergement UE — chiffré TLS	Sessions, comptes, méta-données
Base de données (PostgreSQL)	Hébergement UE — chiffré au repos	Comptes, équipes, liens, sessions
Stockage fichiers (S3)	AWS S3 — région eu-west-3 (Paris) ■■	Fichiers téléchargés par utilisateurs
Email transactionnel	SMTP du client (choix utilisateur)	Adresses email, liens magiques
SMS transactionnel	SMS.to (UE — Chypre) ■■	Numéros de téléphone des destinataires
IA / Modèles linguistiques	OpenAI (US — SCC + DPF)	Textes de transcription/résumés (éphémères)
Authentification	NextAuth.js (auto-hébergé)	Tokens JWT, bcrypt password hash

Point critique — Serveur TURN Hostinger France : Le serveur TURN agit comme un simple *relais réseau chiffré* lorsque la connexion P2P directe est impossible (NAT symétrique). Les flux vidéo sont chiffrés de bout-en-bout via **DTLS-SRTP** : même l'opérateur du TURN ne peut pas voir le contenu vidéo. Aucune donnée vidéo n'est jamais enregistrée sur le serveur.

3. Données personnelles traitées

Catégories de données et finalités

Catégorie	Données	Finalité	Base légale	Conservation
Compte utilisateur	Email, nom, mot de passe (hash bcrypt)	Authentification, gestion de compte	Exécution du contrat	Durée du compte + 30j
Organisation (tenant)	Nom équipe, IP de création, plan	Multi-tenant, anti-abus	Intérêt légitime	Durée du compte
Liens de streaming	Token, créateur, statut, viewers	Établir la session WebRTC	Exécution du contrat	Auto-purge après expiration
Flux vidéo/audio	Caméra smartphone, micro	Diagnostic visuel à distance	Consentement explicite	Non stocké (live uniquement)
Transcription audio (IA)	Texte issu de la voix	Génération résumé de session	Consentement (toggle)	Éphémère (mémoire LLM)
Résumés de session	Texte généré par IA	Documentation pour le technicien	Exécution du contrat	Durée du compte
Logs techniques	IP, user-agent, timestamps	Sécurité, anti-abus, debug	Intérêt légitime	90 jours max
Cookies	Cookie de session NextAuth	Maintien de la session	Strictement nécessaire	7 jours

Note importante : Aucune donnée biométrique, donnée de santé, orientation politique, religieuse ou sexuelle (données sensibles, Art. 9 RGPD) n'est traitée. VisionLink est destiné à un usage **professionnel** (support technique, électroménager, IT, terrain).

4. Mesures techniques de sécurité (Art. 32 RGPD)

Chiffrement

- **HTTPS/TLS 1.2+** imposé sur le domaine vlink.space.
- **HSTS** activé via header Strict-Transport-Security: max-age=31536000; includeSubDomains; preload.
- **WebRTC chiffré bout-en-bout** via **DTLS-SRTP** (obligatoire selon spec RFC 8826).
- **Mots de passe** stockés en **bcrypt** (jamais en clair, salt unique).
- **Base de données** chiffrée au repos (AES-256 côté hébergeur).
- **S3 / fichiers uploadés** : chiffrement SSE-S3 (AES-256) au repos.
- **Liens magiques** : tokens cryptographiques aléatoires (32 octets), expiration 5 min.

Contrôle d'accès

- **Multi-tenant strict** : chaque organisation est isolée logiquement en BDD (filtre tenantId systématique).
- **Sessions JWT** NextAuth signées, durée 7 jours, renouvelables.
- **Middleware d'authentification** sur toutes les routes /dashboard, /admin, /upgrade.
- **Rôles** : owner / member / superadmin avec contrôles distincts.
- **Blocage de tenant** automatique en cas d'abus.

Anti-abus & sécurité applicative

- **Rate limiting** par IP sur : login (10/min), signaling (120/min), notifications (60/min).
- **Limite IP par tenant** : un seul tenant créé par adresse IP.
- **Permissions-Policy** stricte : caméra, micro, géoloc bloqués sauf consentement.
- **X-DNS-Prefetch-Control**, **HSTS preload**, **X-Frame-Options** (CSP-like).
- **Validation et assainissement** systématique des entrées utilisateur.
- **Logs de sécurité** : tentatives login échouées, créations tenant, accès admin.

Anti-fuite de données vidéo

Le flux vidéo n'est JAMAIS enregistré sur les serveurs VisionLink. WebRTC établit une connexion **peer-to-peer** directe entre le smartphone client et le navigateur du technicien. Lorsque le NAT empêche le P2P direct (~15 % des cas), le serveur TURN agit comme un simple **relais réseau chiffré** : il ne fait que transporter des paquets DTLS/SRTP déjà chiffrés, sans pouvoir les déchiffrer ni les stocker. Cela est validé par les normes IETF RFC 5766 (TURN) et RFC 8826 (sécurité WebRTC).

5. Droits des personnes concernées (Art. 12-22 RGPD)

Tout utilisateur ou personne dont les données sont traitées par VisionLink dispose des droits suivants, exerçables par simple email à **contact@vlink.space** :

Droit	Article RGPD	Modalité d'exercice
Droit d'accès	Art. 15	Export JSON/PDF des données — délai 30 jours
Droit de rectification	Art. 16	Modification directe dans le tableau de bord
Droit à l'effacement	Art. 17	Suppression complète du compte sur demande
Droit à la limitation	Art. 18	Suspension du traitement sur demande
Droit à la portabilité	Art. 20	Export JSON structuré
Droit d'opposition	Art. 21	Désactivation des résumés IA possible (toggle)
Décisions automatisées	Art. 22	Aucune décision purement automatisée
Droit de plainte CNIL	Art. 77	www.cnil.fr en cas de litige

Consentement

• **Caméra et micro** : consentement explicite via prompt navigateur (obligatoire, non contournable techniquement).
• **Résumés IA** : opt-in dans les paramètres tenant (toggle *aiSummaryEnabled*).
• **Cookies** : uniquement strictement nécessaires (session), pas de cookie de tracking marketing — aucune bannière de consentement requise.

6. Sous-traitants (Art. 28 RGPD)

Liste complète des sous-traitants traitant des données personnelles pour le compte de VisionLink :

Sous-traitant	Pays / Région	Rôle	Garanties RGPD
Hostinger International Ltd.	VPS France ■■	Serveur TURN/relais WebRTC	DPA RGPD signé, ISO 27001
SMTP client (au choix)	Selon fournisseur choisi	Email transactionnel	Configurable par l'utilisateur
SMS.to	Chypre ■■ (UE)	SMS transactionnel	Société UE, RGPD natif
Xirsys	UE / Royaume-Uni	TURN backup	SCC en place
ExpressTurn	UE	TURN backup	Hébergement UE
AWS (Amazon Web Services)	Région eu-west-3 (Paris)	S■■kage S3 fichiers	DPA + SCC + Data Privacy Framework
OpenAI	États-Unis (SCC + DPF)	Modèles IA (transcription, résumés)	SCC signées, Data Privacy Framework, données non util

Transferts hors UE : seul OpenAI et certains nœuds CDN AWS impliquent un transfert potentiel hors UE. Ces transferts sont encadrés par les **Clauses Contractuelles Types (SCC) 2021** de la Commission européenne et le **Data Privacy Framework UE-US**.

7. Prévention des fuites de données

Pratiques mises en place

• **Aucune clé secrète exposée côté client** : toutes les clés API (SMTP, AWS, Xirsys, SMS.to, OpenAI) restent côté serveur dans des variables d'environnement.

• **Isolation multi-tenant** : impossible pour un utilisateur d'accéder aux données d'une autre organisation (filtre tenantId dans toutes les requêtes Prisma).

• **Liens d'invitation à usage unique** : un lien de stream consommé devient invalide.

• **Auto-purge des sessions** : les liens inactifs sont nettoyés après 15 min (heartbeat manquant).

• **Pas de log de contenu vidéo/audio** : seules les méta-données (timestamps, durée) sont conservées.

• **Headers de sécurité** : HSTS, Permissions-Policy, X-DNS-Prefetch-Control configurés via middleware.

• **Validation stricte des entrées** : sanitizeInput, sanitizeEmail sur toutes les routes API.

• **Rate limiting par IP** sur les endpoints sensibles (auth, signup, signaling).

• **Pas de cookie tiers**, pas de pixel de tracking, pas d'analytics externes type Google Analytics.

• **Communications WebRTC chiffrées de bout-en-bout** (DTLS-SRTP) — même VisionLink ne peut pas voir le contenu vidéo.

Procédure en cas de violation (Art. 33-34 RGPD)

En cas de violation de données personnelles susceptible d'engendrer un risque pour les droits et libertés des personnes :

• **Notification CNIL** dans les **72 heures** à compter de la prise de connaissance.

• **Information des personnes concernées** par email si risque élevé.

• **Documentation** de la violation dans un registre interne dédié.

• **Mesures correctives** immédiates : révocation des tokens, rotation des secrets, audit.

8. Registre des activités de traitement (Art. 30 RGPD)

Conformément à l'article 30 du RGPD, Techmaverick Ltd tient un registre interne des activités de traitement effectuées pour le compte de la plateforme VisionLink. Synthèse publique :

Traitement	Finalité	Catégories de personnes	Base légale	Destinataires
Gestion des comptes	Authentification, gestion d'équipe	Clients pros, techniciens	Contrat	Interne uniquement
Sessions de support vidéo	Diagnostic visuel à distance	Clients finaux du technicien	Consentement	Technicien désigné
Résumés IA	Documentation de session	Clients pros	Consentement (opt-in)	OpenAI (sous SCC/DPF)
Email/SMS transactionnels	Envoi de liens d'invitation	Destinataires invités	Contrat	SMTP client / SMS.to
Logs techniques	Sécurité, anti-abus	Tous utilisateurs	Intérêt légitime	Interne (90j)
Facturation / abonnement	Gestion commerciale	Clients pros	Contrat / obligation légale	Interne

Le registre détaillé complet (durées de conservation par champ, mesures techniques par traitement, transferts hors UE par finalité) est tenu en interne par Techmaverick Ltd et tenu à la disposition de l'autorité de contrôle (CNIL) sur demande.

9. Conclusion

VisionLink présente une **architecture techniquement conforme au RGPD** avec des choix d'hébergement européen privilégiant la souveraineté des données (Hostinger France, AWS Paris, SMS.to UE). L'IA (OpenAI) opère sous SCC et Data Privacy Framework, sans utilisation des données pour entraînement. Le flux vidéo est chiffré de bout-en-bout et jamais enregistré. La politique de confidentialité, les CGU et le registre des traitements sont publiés ou tenus à jour ; les droits des personnes (accès, portabilité, effacement) sont matérialisés dans l'interface (boutons d'export et de suppression).

Aucune fuite de données technique n'a été identifiée. Les mesures de chiffrement, d'isolation multi-tenant, de rate limiting et de validation des entrées constituent une base solide de sécurité.

Document généré automatiquement à des fins d'information. Pour une certification formelle, consulter un DPO externe ou un cabinet juridique spécialisé en protection des données.