DOCUMENT DE SÉCURITÉ

Politique de sécurité des systèmes d'information

La présente Politique de Sécurité des Systèmes d'Information (PSSI) formalise les mesures techniques, physiques et organisationnelles mises en œuvre par Lexia France pour garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données traitées dans le cadre du service SaaS Gilbert.

Security & Privacy by Design
La sécurité est intégrée dès la conception de l'architecture logicielle.

Souveraineté et maîtrise des traitements
Les données sont traitées en priorité au sein de l'Union européenne, sous le contrôle de Lexia.

Émetteur	Lexia France SAS, éditeur de Gilbert
Version	Septembre 2026
Classification	Publique, diffusion clients et partenaires
Délégué à la protection des données	Mathis Escriva
Contact	contact@lexiapro.fr

Sommaire

01 Souveraineté technologique et localisation des données

02 Sécurité logique et chiffrement

03 Politique de minimisation et cycle de vie des données

04 Gestion des accès et des habilitations (IAM)

05 Audit, tests d'intrusion et amélioration continue

06 Résilience, sauvegardes et gestion des incidents

07 Sécurité organisationnelle et humaine

08 Protection des données personnelles (RGPD)

09 Sous-traitants et fournisseurs

10 Réversibilité et fin de contrat

11 Gouvernance de l'intelligence artificielle

12 Dispositions générales

01 Souveraineté technologique et localisation des données

Hébergement des données

L'intégralité des données (fichiers audio, transcriptions, synthèses, métadonnées, bases de données et sauvegardes) est stockée exclusivement dans des infrastructures situées en France ou au sein de l'Union européenne, opérées notamment par OVH SAS et par les fournisseurs techniques utilisés dans le cadre du service Gilbert.

Souveraineté des modèles d'IA

Les modèles d'IA utilisés pour la fourniture du service s'exécutent sur des infrastructures souveraines opérées par Lexia ou par ses sous-traitants souverains (Mistral, OVH), au sein de l'Union européenne. Dans le cadre de l'exécution normale du service, aucun contenu (audio, transcription, synthèse) n'est transmis à des services d'intelligence artificielle publics, à des tiers non autorisés ou à des services d'IA situés hors de l'Union européenne (OpenAI, Anthropic, AWS, Google, Microsoft).

L'architecture technique retenue est conçue pour favoriser le respect des exigences réglementaires applicables, notamment celles du Règlement (UE) 2024/1689 relatif à l'intelligence artificielle (AI Act).

Propriété des données et non-entraînement

Lexia s'interdit d'utiliser les données de ses clients (fichiers audio, transcriptions ou contenus générés) pour entraîner, ajuster ou améliorer des modèles d'intelligence artificielle, génériques ou propriétaires, sans l'accord écrit préalable du Client (opt-in).

02 Sécurité logique et chiffrement

Chiffrement des flux

Tous les échanges entre les terminaux des utilisateurs et la plateforme Gilbert sont chiffrés via TLS 1.3, avec activation systématique de HSTS (HTTP Strict Transport Security).

Stockage et sauvegardes

- Données hébergées sur des serveurs dédiés OVH en France (Lille), sur disques redondés (RAID), dans un datacenter sécurisé.
- Accès à l'infrastructure soumis à un contrôle strict : habilitations minimales, bastion, double facteur d'authentification.
- Sauvegardes chiffrées en AES-256, avec des clés gérées par Lexia ; l'hébergeur n'a pas accès à ces clés.

Cloisonnement logique (multi-tenant)

Les données de chaque client sont isolées de manière étanche au niveau applicatif et au niveau de la base de données : aucun utilisateur d'une organisation ne peut accéder aux données d'une autre organisation.

Minimisation des données audio

L'enregistrement audio brut fourni pour transcription est automatiquement et définitivement supprimé des serveurs de production dans un délai maximal de 24 heures après la génération de la transcription.

03 Politique de minimisation et cycle de vie des données

Lexia applique une politique stricte de suppression en cascade afin de réduire au maximum la surface d'exposition aux risques.

Catégorie de données	Durée de conservation	Action post-délai
Fichiers audio bruts	24 heures maximum après transcription	Suppression automatique et irréversible
Transcriptions et synthèses	Durée de vie du compte actif	Effacement immédiat à la demande du Client
Sauvegardes	30 jours	Élimination définitive par rotation automatique
Journaux de connexion et d'activité	12 mois	Purge automatique ou anonymisation

Ces durées peuvent être adaptées lorsqu'une obligation légale, réglementaire ou judiciaire l'exige.

04 Gestion des accès et des habilitations (IAM)

Authentification forte

- Prise en charge native du double facteur d'authentification (2FA).
- Authentification unique (SSO, OAuth 2.0) via Microsoft Entra ID et Google Workspace.

Contrôle des accès internes

- L'accès à l'infrastructure de production est limité aux seules personnes habilitées.
- Les interventions techniques s'effectuent via des bastions sécurisés à double facteur.
- Toutes les opérations sensibles font l'objet d'une journalisation sécurisée et horodatée, conservée 12 mois.

05 Audit, tests d'intrusion et amélioration continue

- **Audit de conformité client.** Lexia permet à ses clients de mener un (1) audit de sécurité par an, réalisé par un auditeur tiers indépendant mandaté et rémunéré exclusivement par le Client. Cet audit est soumis à un préavis minimal de trente (30) jours ouvrés et doit être confié à un professionnel indépendant, qui n'est pas un concurrent direct de Lexia et qui est préalablement soumis à un accord de confidentialité. Lexia s'engage à collaborer activement et gratuitement à cet audit, dans la limite d'un volume raisonnable d'assistance technique.
- **Tests d'intrusion.** Lexia fait réaliser un test d'intrusion externe annuel, confié à un cabinet indépendant spécialisé en cybersécurité, afin d'identifier et de corriger d'éventuelles vulnérabilités applicatives (OWASP Top 10).
- **Correctifs et mises à jour.** Les serveurs et les dépendances logicielles font l'objet d'une veille de sécurité active et de l'application régulière des correctifs de sécurité.

Lexia maintient un processus continu de veille, d'identification, d'évaluation et de correction des vulnérabilités susceptibles d'affecter les composants applicatifs ou d'infrastructure participant à la fourniture du service.

06 Résilience, sauvegardes et gestion des incidents

Politique de sauvegarde

Les sauvegardes sont quotidiennes, chiffrées en AES-256 et répliquées de manière sécurisée dans une zone géographique distincte d'OVH. Des tests de restauration sont menés chaque mois.

Objectifs de résilience (PCA)

Objectif	Valeur	Portée
RPO (point de récupération)	24 heures maximum	Perte de données maximale théorique
RTO (temps de restauration)	4 heures maximum	Objectif de moyens pour rétablir la disponibilité, hors force majeure ou défaillance systémique de l'hébergeur

Notification des incidents

En cas d'incident ou de violation de données à caractère personnel, Lexia informe le Client dans les meilleurs délais, et au plus tard 24 heures après qualification. Cette notification contient toutes les informations nécessaires pour permettre au Client de remplir ses obligations réglementaires auprès de la CNIL sous 72 heures.

07 Sécurité organisationnelle et humaine

- **Engagements de confidentialité.** Tous les salariés et collaborateurs de Lexia sont contractuellement soumis à des obligations strictes de confidentialité et de secret professionnel.
- **Sensibilisation interne.** Les équipes de développement sont formées en continu aux principes du codage sécurisé et sensibilisées aux techniques d'ingénierie sociale (hameçonnage).

08 Protection des données personnelles (RGPD)

- Le Client agit en qualité de responsable de traitement.
- Lexia agit en qualité de sous-traitant pour les traitements réalisés pour le compte du Client.

Lexia met en œuvre des mesures techniques et organisationnelles appropriées, destinées à garantir un niveau de sécurité adapté aux risques, conformément à l'article 32 du RGPD. Lexia assiste le Client, dans une mesure raisonnable et proportionnée, dans le respect de ses obligations relatives à la protection des données personnelles.

09 Sous-traitants et fournisseurs

Les fournisseurs sont sélectionnés selon des critères incluant notamment la sécurité, la confidentialité, la conformité réglementaire et la qualité de service. Les sous-traitants intervenant dans la fourniture du service sont soumis à des obligations contractuelles appropriées en matière de protection des données et de sécurité. Tout transfert international éventuel de données personnelles est encadré conformément au RGPD.

10 Réversibilité et fin de contrat

À l'expiration du contrat :

- le Client peut demander la restitution de ses données dans un format raisonnablement exploitable ;
- les données sont supprimées ou anonymisées conformément à la politique de conservation ;
- les obligations légales de conservation demeurent applicables lorsqu'elles existent.

11 Gouvernance de l'intelligence artificielle

Les fonctionnalités d'intelligence artificielle intégrées à la plateforme Gilbert sont des outils d'assistance à la transcription, à l'analyse et à la synthèse d'informations. Les résultats générés peuvent comporter des erreurs, des approximations ou des omissions. Le Client demeure seul responsable des décisions prises sur la base des informations produites par la plateforme ; une validation humaine appropriée est recommandée avant toute prise de décision.

12 Dispositions générales

La présente PSSI est un document descriptif des mesures de sécurité mises en œuvre par Lexia. En cas de contradiction avec les documents contractuels applicables, les dispositions contractuelles prévalent.

Les mesures décrites peuvent évoluer pour tenir compte de l'évolution des menaces, des technologies, des exigences réglementaires et de l'état de l'art. Malgré la mise en œuvre de mesures techniques et organisationnelles adaptées, aucun système d'information ne peut garantir une protection absolue contre l'ensemble des risques existants ou futurs. Les mesures décrites constituent une obligation de moyens et non une garantie de résultat.

Questions de sécurité et exercice des droits : contact@lexiapro.fr.