

Accord de traitement des données (DPA) - VOOK SAS

Version 2026-09

Cadre du DPA

Le présent accord de traitement des données (« DPA ») complète les Conditions Générales d'Utilisation de Vook disponibles à l'adresse vook.ai/fr/terms-of-service (le « Contrat »). Il est conclu entre vous et l'entité que vous représentez (« Client », « vous » ou « votre », également désigné le « Responsable de traitement » dans les annexes) et Vook SAS, société par actions simplifiée au capital de 5 000 euros, dont le siège social est situé 10 rue Vandrezanne, 75013 Paris, France, immatriculée au registre du commerce et des sociétés de Paris sous le numéro 980 855 027 (n° de TVA intracommunautaire FR59980855027), agissant en qualité de sous-traitant au sens du règlement (UE) 2016/679 (le « RGPD ») (« Vook »).

L'acceptation des Conditions Générales d'Utilisation de Vook par le Client constitue l'acceptation du présent DPA. Aucune signature n'est requise pour l'entrée en vigueur du présent DPA. La poursuite de l'utilisation du Service vaut acceptation continue.



Préambule

Vook édite et exploite un service de transcription et d'analyse de fichiers audio et vidéo (le « Service »). Le Client utilise le Service, ce qui conduit Vook à traiter des données à caractère personnel pour son compte.

Au sens du règlement (UE) 2016/679 (le « RGPD »), le Client agit en qualité de responsable de traitement et Vook en qualité de sous-traitant. Le présent DPA est conclu en application de l'article 28 du RGPD et régit ce traitement. Il complète le contrat de service principal défini à l'article 10.

Ceci exposé, il a été convenu ce qui suit :

Article 1. Définitions

Les termes « données à caractère personnel », « traitement », « responsable du traitement », « sous-traitant », « sous-traitant ultérieur », « personne concernée », « violation de données à caractère personnel » et « autorité de contrôle » ont le sens que leur donne le RGPD. « Sous-traitant ultérieur » désigne tout tiers auquel Vook fait appel pour traiter des données à caractère personnel au titre du présent DPA. Les « Clauses Contractuelles Types » ou « CCT » désignent les clauses contractuelles types de l'UE adoptées par la décision d'exécution (UE) 2021/914 de la Commission. Sauf mention contraire, les références à des articles (« art. ») dans le présent DPA et ses annexes renvoient aux articles du RGPD.

Article 2. Description du traitement (art. 28(3))

- **Objet** : fourniture du Service au Client.
- **Durée** : pendant la durée du contrat de service principal et jusqu'à la suppression ou la restitution des données à caractère personnel conformément à l'article 8.
- **Nature et finalité** : hébergement, transcription, identification des locuteurs (diarisation), synthèse et chat IA optionnels, stockage et transmission du contenu du Client, aux seules fins de fournir le Service.
- **Types de données à caractère personnel** : données de compte et d'identité (nom, e-mail, identifiants OAuth) ; données de facturation (nom, adresse postale) ;

métadonnées d'usage et techniques (IP, données de requête et de session, titres et noms de fichiers des transcriptions) ; et **contenu du Client** (fichiers audio/vidéo, transcriptions, synthèses, chat), susceptible de contenir des données à caractère personnel et, incidemment, des données de catégories particulières au sein de ce contenu.

- **Catégories de personnes concernées** : les utilisateurs autorisés du Client et toute personne apparaissant dans le contenu téléversé par le Client.
- Détails complets du traitement : Annexe 1, y compris les valeurs des Annexes I à III des CCT.

Article 3. Obligations de Vook (art. 28(3))

Vook s'engage à :

- (a) **Instructions documentées** : ne traiter les données à caractère personnel que sur instructions documentées du Client (y compris pour les transferts), sauf obligation prévue par le droit de l'UE ou d'un État membre ; dans ce cas, Vook informe le Client, sauf interdiction légale. Le présent DPA et l'utilisation du Service par le Client constituent les instructions initiales.
- (b) **Confidentialité** : veiller à ce que les personnes autorisées à traiter les données à caractère personnel soient soumises à une obligation de confidentialité (voir l'Annexe 2 et l'article 5 ci-dessous).
- (c) **Sécurité** : mettre en œuvre les mesures techniques et organisationnelles décrites à l'Annexe 2, conformément à l'art. 32.
- (d) **Sous-traitants ultérieurs** : ne faire appel à des sous-traitants ultérieurs que dans les conditions de l'article 4.
- (e) **Droits des personnes concernées** : aider le Client, par des mesures techniques et organisationnelles appropriées et dans la mesure du possible, à répondre aux demandes des personnes concernées au titre du chapitre III du RGPD (article 7).
- (f) **Assistance** : aider le Client à garantir le respect des art. 32 à 36 (sécurité, notification des violations, analyse d'impact relative à la protection des données (AIPD), consultation préalable), compte tenu de la nature du traitement et des informations à la disposition de Vook.

- (g) **Suppression / restitution** : au choix du Client, supprimer ou restituer les données à caractère personnel au terme de la prestation du Service, conformément à l'article 8 et à l'Annexe 3.
- (h) **Preuves de conformité et audits** : mettre à disposition les informations nécessaires pour démontrer le respect de l'art. 28, et permettre la réalisation d'audits et y contribuer, conformément à l'article 9.

Article 4. Sous-traitants ultérieurs

- Le Client accorde à Vook une autorisation écrite générale de recourir à des sous-traitants ultérieurs. La liste actuelle figure à l'Annexe 4.
- Vook impose à chaque sous-traitant ultérieur, par contrat, des obligations de protection des données équivalentes en substance à celles du présent DPA (art. 28(4)), telles que documentées à l'Annexe 4, et demeure pleinement responsable envers le Client de l'exécution de leurs obligations par ses sous-traitants ultérieurs.
- Vook informe le Client de tout changement envisagé (ajout ou remplacement d'un sous-traitant ultérieur) au moins 30 jours à l'avance, par mise à jour de la liste publique des sous-traitants ultérieurs à l'adresse <https://vook.ai/fr/sub-processors> et, pour les Clients ayant enregistré un contact protection des données auprès de Vook, par e-mail à ce contact. Le Client peut s'y opposer dans ce délai pour des motifs raisonnables tenant à la protection des données et, à défaut d'accord alternatif, résilier son abonnement sans pénalité.

Article 5. Confidentialité

Toutes les personnes (fondateurs ; personnel des sous-traitants ultérieurs) autorisées à accéder aux données à caractère personnel sont tenues à la confidentialité par contrat ou par obligation légale. Au sein de Vook, l'accès à la production est restreint à un administrateur nommé unique (voir l'Annexe 2, §1.1).

Article 6. Transferts internationaux

Le traitement entre les Parties au titre du présent DPA n'implique pas en lui-même de transfert hors de l'UE/EEE : Vook est établie en France, et le stockage principal comme le calcul sont localisés dans l'UE. Les CCT s'appliquent dans deux situations :

- **Transferts ultérieurs vers des sous-traitants ultérieurs.** Lorsqu'un sous-traitant ultérieur listé à l'Annexe 4 est établi hors de l'UE/EEE ou soumis au droit d'un pays tiers, le transfert est régi par les CCT, Module 3 (sous-traitant vers sous-traitant), conclues entre Vook et ce sous-traitant ultérieur via l'accord de traitement des données propre à ce dernier, et complétées par les mesures techniques de l'Annexe 2 (TLS en transit, chiffrement AES-256 par utilisateur du contenu au repos).
- **Cadre de protection des données UE-États-Unis.** Lorsqu'un sous-traitant ultérieur est certifié au titre du cadre de protection des données UE-États-Unis (« DPF »), la décision d'adéquation DPF constitue la base de transfert principale pour les données à caractère personnel transférées vers ce sous-traitant, les CCT s'appliquant à titre de repli. La liste des sous-traitants ultérieurs publiée à l'adresse <https://vook.ai/fr/sub-processors> indique, par sous-traitant, le mécanisme applicable.
- **Clients établis hors de l'UE/EEE.** Lorsque le Client est établi hors de l'UE/EEE, les CCT, Module 4 (sous-traitant vers responsable de traitement), sont incorporées par référence au présent DPA pour les flux de données de Vook vers le Client (y compris l'accès à distance du Client aux données hébergées par Vook), complétées par les valeurs de l'Annexe I des CCT figurant à l'Annexe 1. Pour les Clients établis au Royaume-Uni, l'International Data Transfer Addendum britannique s'applique en complément ; pour les Clients établis en Suisse, les CCT s'appliquent telles qu'adaptées selon les exigences du PFPDT.

Vook documente son évaluation des lois des pays de destination et des mesures supplémentaires (clause 14 des CCT) à l'Annexe 5, annexe informative mise à jour en même temps que la liste des sous-traitants ultérieurs et fournie pour faciliter la propre évaluation des transferts du Client.

Vook ne garantit pas une exclusion totale de tout traitement hors de l'UE/EEE. Le stockage principal et le calcul sont localisés dans l'UE, mais certains sous-traitants ultérieurs sont des sociétés de droit américain, et la synthèse/le chat IA n'envoient du contenu à un prestataire de droit américain que sur action explicite et consentie de l'utilisateur. Sur souscription de l'option « résidence UE » pour la fonction IA, la synthèse et le chat IA sont exécutés sur un point de terminaison situé dans l'UE, de sorte que le contenu envoyé à la fonction IA reste traité dans la géographie UE (voir les Annexes 4 et 5).

Article 7. Droits des personnes concernées et notification des violations

- **Assistance aux droits** : Vook aide le Client à satisfaire les demandes des personnes concernées (accès, rectification, effacement, portabilité, limitation, opposition) au titre du chapitre III, au moyen des fonctionnalités du Service et du support de l'opérateur. L'export et la restitution sont effectués par l'utilisateur via l'export en libre-service intégré au produit, pour une ou plusieurs transcriptions à la fois (PDF/DOCX/SRT/JSON/HTML/MD, chat, audio d'origine ; le format JSON, structuré et lisible par machine, répond à l'exigence de portabilité de l'art. 20 du RGPD). Le contenu est chiffré par utilisateur et ne peut pas être déchiffré par Vook, sauf pour les utilisateurs ayant expressément demandé la conservation d'une clé de récupération, option explicite permettant de restaurer l'accès à leur compte (les titres et noms de fichiers des transcriptions, simples métadonnées, sont en revanche stockés en clair) ; il n'existe donc pas d'extraction du contenu en clair côté opérateur, et la restitution au Client à la résiliation est satisfaite par l'export en libre-service de ses utilisateurs (voir l'Annexe 3, §2).
- **Violation de données à caractère personnel** : Vook notifie le Client sans retard injustifié, et en tout état de cause dans les 48 heures suivant la prise de connaissance d'une violation de données à caractère personnel affectant les données du Client, avec les informations disponibles, et coopère à la remédiation et aux obligations du Client au titre des art. 33 et 34.

Article 8. Suppression et restitution

À la fin du Service, Vook supprime ou restitue les données à caractère personnel du Client conformément à l'Annexe 3, sous réserve des obligations légales de conservation (factures, 10 ans) et de la fenêtre de rotation des sauvegardes. La suppression est achevée dans les 30 jours suivant la demande et confirmée par écrit au Client.

Article 9. Audits

- (a) **Informations.** Vook met à la disposition du Client toutes les informations nécessaires pour démontrer le respect de l'art. 28 du RGPD : le présent DPA et ses annexes, la documentation des mesures techniques et organisationnelles (Annexe 2), la liste des sous-traitants ultérieurs et l'état du DPA de chacun d'eux (Annexe 4), l'évaluation des transferts (Annexe 5), ainsi que les certifications publiées par ses sous-traitants ultérieurs d'infrastructure. Vook répond en outre à un

questionnaire écrit de sécurité/conformité du Client par période de 12 mois, sous 30 jours.

(b) **Audit (documentation d'abord).** Les demandes d'audit sont satisfaites en premier lieu par la documentation visée au (a). Lorsque le Client démontre raisonnablement que cette documentation est insuffisante, ou à la suite d'une violation de données à caractère personnel affectant ses données, ou lorsqu'une autorité de contrôle l'exige, le Client (ou un auditeur indépendant qu'il mandate, qui ne doit pas être un concurrent de Vook et doit être tenu à la confidentialité) peut auditer le respect du présent DPA par Vook, dans les conditions suivantes :

- au plus une fois par période de 12 mois (cette limite ne s'applique pas après une violation affectant les données du Client, ni lorsqu'une autorité de contrôle l'exige) ;
- préavis écrit de 30 jours, avec périmètre et durée convenus à l'avance ;
- audit mené à distance par défaut, pendant les heures ouvrées, limité à un jour ouvré, sans perturber de manière déraisonnable les opérations de Vook ;
- périmètre limité à ce qui est nécessaire pour vérifier le respect du présent DPA à l'égard des données à caractère personnel du Client. Il ne s'étend pas : (i) aux données des autres clients, que l'auditeur ne peut de toute façon pas lire puisque le contenu est chiffré par utilisateur (Annexe 2) ;
(ii) aux informations financières internes de Vook ; (iii) aux audits directs des sous-traitants ultérieurs ; pour ceux-ci, Vook fournit les certifications et rapports d'audit du sous-traitant ultérieur disponibles au titre de son propre DPA (Annexe 4).

(c) **Coûts.** Chaque Partie supporte ses propres coûts ; le Client supporte les honoraires de son auditeur. L'assistance de Vook au-delà d'un jour ouvré par période de 12 mois peut être facturée à ses tarifs standards, sauf si l'audit révèle un manquement substantiel de Vook au présent DPA, auquel cas Vook supporte ses propres coûts d'assistance.

(d) **Conclusions.** Les résultats d'audit sont confidentiels, sont communiqués à Vook et ne peuvent être utilisés que pour vérifier le respect du présent DPA et y remédier. Vook remédie à tout manquement confirmé selon un plan de remédiation convenu sans retard injustifié.

Article 10. Responsabilité, durée, droit applicable, hiérarchie

- **Contrat principal.** Lorsque les Parties n'ont pas signé de contrat-cadre de services distinct, le « contrat de service principal » désigne les Conditions Générales de Vook ainsi que le devis ou bon de commande accepté par le Client. Le présent article 10 est autonome afin de s'appliquer pleinement dans cette configuration. L'acceptation des Conditions Générales d'Utilisation de Vook par le Client constitue l'acceptation du présent DPA dans son intégralité.
- **Durée.** Le présent DPA s'applique aussi longtemps que Vook traite des données à caractère personnel pour le compte du Client et survit pour les obligations de suppression et de restitution (article 8).
- **Responsabilité envers les personnes concernées (art. 82 RGPD).** Régime légal, non affecté par le présent DPA : Vook n'est responsable envers les personnes concernées du dommage causé par le traitement que s'il n'a pas respecté les obligations du RGPD incombant spécifiquement aux sous-traitants, ou s'il a agi en dehors des instructions licites du Client ou contrairement à celles-ci.
- **Recours entre les Parties (art. 82(5)).** Lorsqu'une Partie a réparé intégralement le dommage subi par une personne concernée, elle est en droit de réclamer à l'autre Partie la part de la réparation correspondant à la part de responsabilité de cette autre Partie dans le dommage.
- **Amendes administratives.** Chaque Partie supporte les amendes administratives qui lui sont infligées par une autorité de contrôle.
- **Plafond de responsabilité.** La responsabilité totale cumulée de chaque Partie envers l'autre au titre ou à l'occasion du présent DPA, toutes demandes et causes confondues, est limitée au total des montants payés ou dus par le Client pour le Service au cours des douze (12) mois précédant le fait générateur de responsabilité.
- **Exclusion des dommages indirects.** Aucune Partie n'est responsable envers l'autre des dommages indirects ou consécutifs, y compris la perte de profits, de revenus, d'activité, de clientèle ou d'économies escomptées.
- **Réserves impératives.** Rien dans le présent DPA ne limite ni n'exclut la responsabilité d'une Partie en cas de dol ou de faute lourde, de dommage corporel, ou pour toute autre responsabilité ne pouvant être limitée ou exclue en vertu du droit applicable.

- **Droit applicable / juridiction.** Le présent DPA est régi par le droit français. Tout litige relatif à sa validité, son interprétation ou son exécution relève des tribunaux du ressort de la cour d'appel de Paris.
- **Ordre de priorité (questions de protection des données).** Les CCT prévalent sur le présent DPA, qui prévaut sur le contrat de service principal.

Annexes

Les annexes suivantes font partie intégrante du présent DPA :

- **Annexe 1 :** description du traitement et valeurs des Annexes I à III des CCT ;
- **Annexe 2 :** mesures techniques et organisationnelles ;
- **Annexe 3 :** suppression et restitution des données ;
- **Annexe 4 :** liste des sous-traitants ultérieurs ;
- **Annexe 5 :** analyse d'impact des transferts (annexe informative, mise à jour avec l'Annexe 4 selon le mécanisme de l'article 4).

Annexe 1 : Description du traitement (art. 28(3) RGPD)

Vook agit en qualité de **sous-traitant** (art. 28 RGPD) ; le client est **responsable de traitement**. Cette annexe décrit le traitement confié à Vook ; elle détermine le périmètre des instructions documentées du responsable de traitement.

1. Objet du traitement

Fourniture au Responsable de traitement du service Vook de transcription, diarisation (identification des tours de parole), résumé et analyse assistés par IA de fichiers audio et vidéo (le « Service »).

2. Durée du traitement

La durée du contrat de service principal, puis jusqu'à la suppression ou la restitution des données à caractère personnel conformément à la clause « Suppression et restitution » du DPA (suppression achevée dans les 30 jours de la demande et confirmée par écrit ; voir l'Annexe 3).

3. Nature du traitement

Opérations réalisées, exclusivement pour fournir le Service :

- **collecte** : téléversement des fichiers audio/vidéo par les utilisateurs du Responsable de traitement ;
- **hébergement et stockage chiffré** : le contenu (audio, transcriptions, résumés, chat) est chiffré AES-256 sous clés propres à chaque utilisateur avant stockage ; Vook ne détient pas de clé permettant de le déchiffrer côté serveur, sauf lorsque l'utilisateur a expressément demandé la conservation d'une clé de récupération (option explicite) ; les titres et noms de fichiers des transcriptions, simples métadonnées, sont stockés en clair ;
- **transcription et diarisation, exécutées sur des serveurs GPU situés dans l'UE/EEE**, de manière éphémère : les données ne sont déchiffrées qu'en mémoire, le temps de l'inférence, puis rejetées ;

- **résumé, analyse et chat IA, optionnels** : déclenchés uniquement par une action explicite de l'utilisateur, après une notice de consentement à la première utilisation ; jamais de façon automatique sur l'ensemble des contenus ;
- **consultation et export** par l'utilisateur (transcriptions : PDF, DOCX, SRT, JSON, HTML, Markdown ; chat : PDF, DOCX, Markdown ; audio d'origine) ;
- **transmission** strictement nécessaire à la fourniture du Service ;
- **effacement** : suppression à la demande, par élément ou par compte (voir Annexe 3).

4. Finalité du traitement

Exclusivement la fourniture du Service au Responsable de traitement. Aucune utilisation à des fins publicitaires, aucun profilage, et **aucun entraînement de modèles d'IA sur les données du Responsable de traitement** (voir §9).

5. Catégories de données à caractère personnel

- **données de compte / d'identité** : nom, adresse e-mail, identifiants OAuth ;
- **données de facturation** : nom, adresse postale (collectées uniquement à l'achat) ;
- **métadonnées d'usage et techniques** : adresse IP, données de requête/session, événements produit, titres et noms de fichiers des transcriptions (stockés en clair)
- **contenu du Responsable de traitement** : fichiers audio/vidéo, transcriptions, résumés, conversations (chat), susceptibles de contenir toute donnée personnelle figurant dans la parole enregistrée, y compris, de manière incidente, des catégories particulières de données (art. 9).

6. Données sensibles et qualification de la voix

- **Catégories particulières (art. 9)** : elles ne sont ni demandées ni traitées intentionnellement par Vook ; elles peuvent être incidemment contenues dans les contenus du Responsable de traitement (par exemple pour des usages santé ou juridique). Il appartient au Responsable de traitement de s'assurer de la licéité de

leur traitement (base art. 9(2)) ; Vook applique les garanties suivantes : chiffrement par utilisateur au repos (Vook ne détient pas de clé de déchiffrement, sauf option de récupération expressément demandée par l'utilisateur), TLS en transit, limitation stricte de finalité, stockage et inférence de transcription dans l'UE, isolation des données par utilisateur.

- **Voix et données biométriques** : les enregistrements vocaux sont traités pour la transcription et la diarisation, et non aux fins d'identifier une personne physique de manière unique. La diarisation distingue les locuteurs au sein d'un même fichier (« Locuteur A », « Locuteur B ») de manière éphémère ; Vook ne constitue **aucun gabarit biométrique persistant** ni aucune base de référence de voix permettant de reconnaître une personne d'un fichier à l'autre. Le traitement ne relève donc pas des données biométriques au sens de l'art. 9(1) RGPD.

7. Catégories de personnes concernées

- les utilisateurs autorisés du Responsable de traitement (titulaires de comptes) ;
- toute personne enregistrée, mentionnée ou identifiable dans les contenus téléversés (locuteurs, participants aux réunions, tiers cités).

8. Durées de conservation

Données	Durée
Contenu (audio, transcriptions, résumés, chat)	Jusqu'à suppression par l'utilisateur / le Responsable de traitement, ou clôture du compte ; effacement selon l'Annexe 3
Données de compte	Durée du compte ; anonymisation à la clôture
Comptes inactifs	Suppression automatique après deux (2) ans d'inactivité, après notification préalable ; même effacement que l'Annexe 3
Empreinte (hash) de l'e-mail d'un compte supprimé	12 mois (prévention de la ré-inscription abusive, intérêt légitime), puis suppression
Événements analytiques	13 mois maximum (TTL natif au niveau de la table), puis agrégats anonymes uniquement
Factures	10 ans (obligation légale : Code de commerce, art. L123-22)
Sauvegardes	Rotation de 30 jours ; le crypto-effacement rend les résidus illisibles immédiatement
Journaux techniques (logs)	15 jours

En fin de contrat : suppression ou restitution, au choix du Responsable de traitement ; la restitution s'effectue par l'export en libre-service des utilisateurs (le contenu étant chiffré par utilisateur, il n'existe pas d'extraction en clair côté opérateur ; propriété de confidentialité volontaire). Suppression achevée sous 30 jours et confirmée par écrit.

9. Engagement relatif aux modèles d'IA

- La transcription et la diarisation s'exécutent sur l'infrastructure pilotée par Vook, sur des serveurs GPU situés dans l'UE/EEE, de manière éphémère ;
- les résumés et le chat utilisent Google Gemini au palier payant, dont les conditions excluent l'utilisation des contenus soumis pour améliorer les modèles ; le contenu n'y est envoyé que sur action explicite et consentie de l'utilisateur (par défaut sur un point de terminaison global ; sur option payante, sur un point de terminaison UE) ;
- **aucune donnée du Responsable de traitement** (audio, vidéo, transcriptions, résumés, données d'usage) **n'est utilisée pour entraîner, affiner ou améliorer un quelconque modèle d'IA**, ni par Vook ni par ses sous-traitants ultérieurs.

10. Localisation du traitement

Le stockage primaire et le calcul applicatif s'exécutent dans l'UE, à Paris, chez Scaleway, prestataire français certifié ISO 27001, SOC 2 et HDS (Hébergeur de Données de Santé). Ces certifications sont celles de l'hébergeur : **Vook ne détient pas de certification propre** (ni ISO 27001, ni SOC 2, ni HDS). L'inférence de transcription s'exécute sur des serveurs GPU situés dans l'UE/EEE.

Certaines fonctions spécifiques (paiement, e-mail transactionnel, connexion OAuth, observabilité, et la fonction optionnelle de résumé/chat IA) font intervenir des sous-traitants ultérieurs établis hors UE/EEE, encadrés par les Clauses Contractuelles Types ; voir la liste des sous-traitants ultérieurs (Annexe 4) et la clause « Transferts internationaux » du DPA. Le contenu du Responsable de traitement (audio, transcriptions, résumés, chat) ne transite jamais par le prestataire d'e-mail transactionnel ni par l'hébergeur frontend ; ces prestataires ne reçoivent respectivement que des adresses e-mail/contenus d'e-mails et des données de compte/session. **Vook ne garantit pas une exclusivité UE/EEE absolue** et documente honnêtement ces points de contact (position constante ; voir l'article 6 du DPA).

Option « résidence UE » pour la fonction IA (payante). Sur souscription de cette option, les résumés et le chat IA sont exécutés sur un point de terminaison situé dans l'UE (Vertex AI, multi-région UE), de sorte que le contenu envoyé à la fonction IA reste traité dans la géographie UE. L'activation est effectuée pour le compte du Responsable de traitement lors de la souscription.

Annexe 2 : Mesures techniques et organisationnelles (MTO)

Annexe au DPA Vook (art. 28 / art. 32 RGPD). Décrit les mesures techniques et organisationnelles que Vook (sous-traitant) maintient pour protéger les données à caractère personnel traitées pour le compte du responsable de traitement.

0. Vue d'ensemble

Vook est opéré par une équipe de trois fondateurs, sans salariés ni prestataires externes. L'infrastructure de production est entièrement hébergée dans le cloud, dans l'UE. L'accès à la production est restreint à un administrateur nommé unique. Les mesures ci-dessous suivent la structure de l'art. 32(1) du RGPD.

1. Confidentialité

1.1 Contrôle d'accès

- **Comptes nominatifs** sur chaque service ; aucun compte partagé (à l'exception de la boîte support contact@vook.ai, partagée par les trois fondateurs).
- **2FA** imposée sur tous les comptes d'administration.
- **Accès à la production restreint à un administrateur nommé unique.** Les autres fondateurs n'ont accès qu'à l'environnement de développement.
- **Isolation réseau de la base de données :** l'instance PostgreSQL de production n'a pas d'IP publique et n'est joignable que via un réseau privé ; il n'existe aucun point d'accès public.
- **Analytics :** accès par identifiant nominatif propre à chaque fondateur, via HTTPS.

1.2 Chiffrement

- **En transit :** TLS/HTTPS imposé sur tous les services exposés à Internet (vook.ai et l'API backend). HTTP est redirigé vers HTTPS (force_https) ; les certificats sont émis et renouvelés automatiquement par les hébergeurs (Let's Encrypt / gérés par le fournisseur).
- **Au repos :** les contenus utilisateur (fichiers audio, transcriptions, artefacts dérivés) sont chiffrés en AES-256 avant stockage, avec un matériel de clé propre à chaque utilisateur. Les titres et noms de fichiers des transcriptions ne font pas partie du contenu chiffré : ils sont stockés en clair, comme métadonnées (et mis à null à la

suppression du compte). Les mots de passe sont hachés avec bcrypt. Sur demande explicite de l'utilisateur (option de récupération), une copie de sa clé de chiffrement est conservée, enveloppée via Scaleway Key Manager, pour permettre la restauration de l'accès au compte ; à défaut, Vook ne conserve aucune clé permettant de déchiffrer le contenu.

- **Jetons** : chaque type de JWT dispose de son propre secret, séparé entre dev et prod.

1.3 Minimisation des données et pseudonymisation

- Seules les données nécessaires au service sont collectées : inscription = e-mail + mot de passe ; facturation = nom + adresse postale, recueillis uniquement à l'achat ; transcription = audio traité puis résultats stockés, accessibles au seul propriétaire.
- La suppression d'un compte déclenche un pipeline d'effacement complet : profil anonymisé (nom supprimé, e-mail remplacé par un identifiant aléatoire), identifiants d'authentification et clés de chiffrement par utilisateur détruits (crypto-effacement), enregistrements de contenu réduits à des squelettes non personnels et objets stockés supprimés, événements analytics supprimés, abonnement résilié et objet client Stripe effacé. Le pipeline s'achève sous un SLA de 30 jours, avec supervision automatisée.

1.4 Isolation des utilisateurs

- Chaque utilisateur n'accède qu'à ses propres données (isolation par user_id). Transcriptions, audio et données de facturation sont strictement cloisonnés. Il n'existe aucune fonctionnalité de partage public des transcriptions.

2. Intégrité

- **Intégrité du transport** : tout le trafic externe passe par TLS ; le trafic inter-services entre le backend et le processeur audio transite par le réseau privé des fournisseurs.
- **Journalisation et traçabilité** : les opérations sensibles sont journalisées via Datadog avec des catégories structurées (Auth, Admin, Subscription, etc.) et un contexte utilisateur automatique par requête (CLS). Rétention des journaux : 15 jours.

- **Journal d'audit admin** : chaque opération admin modifiante est enregistrée dans un journal d'audit persistant (acteur, action, utilisateur cible, contenu de la requête ; les identifiants de connexion ne sont jamais persistés), appliqué globalement au niveau du framework et non endpoint par endpoint, de sorte qu'aucune mutation admin ne peut le contourner.
- **Contrôle des changements** : toutes les modifications de code passent par Git (GitHub) avec revue par pull request ; les décisions d'architecture sont consignées sous forme d'ADR.

3. Disponibilité et résilience

- **Redondance applicative** : instances applicatives redondantes avec répartition de charge et bascule gérées par le fournisseur.
- **Réplication de la base de données** : l'instance PostgreSQL de production dispose d'un réplica quasi temps réel pour la bascule.
- **Sauvegardes** : sauvegardes PostgreSQL quotidiennes automatisées, stockées dans un stockage objet en UE, avec fenêtre de rétention définie et vérification d'intégrité.
- **Protection contre la suppression du stockage de contenu** : le stockage de contenu utilisateur chiffré comporte des garde-fous qui empêchent toute suppression ou purge silencieuse des contenus.
- **Code source** : hébergé sur GitHub avec l'historique complet.

4. Restauration

- Les données peuvent être restaurées depuis les sauvegardes quotidiennes Scaleway (fenêtre de 30 jours) ou, pour une bascule immédiate, depuis le réplica PostgreSQL. L'analytics est une donnée dérivée, restructurable depuis la base PostgreSQL primaire.

5. Mesures organisationnelles

- **Personnel** : trois fondateurs, ni salariés ni prestataires ; comptes nominatifs ; l'accès à la production est restreint à un administrateur nommé unique.

- **Localisation de l'hébergement** : l'ensemble du calcul et du stockage de production se trouve dans l'UE. La consolidation UE sur Scaleway est réalisée pour l'hébergement applicatif, le stockage et la gestion des clés.
- **Sous-traitants ultérieurs** : régis par l'annexe dédiée aux sous-traitants ultérieurs (Annexe 4) ; engagés sous le DPA de chaque fournisseur, complété par les CCT le cas échéant.
- **Développement sécurisé** : protection des données dès la conception (minimisation des données, isolation des utilisateurs, chiffrement) ; séparation des secrets dev/prod ; revue de code ; ADR.
- **Traitement des données chez les sous-traitants ultérieurs** : l'inférence GPU (RunPod) traite des entrées chiffrées et restitue des sorties chiffrées, s'exécute dans l'UE/EEE et est éphémère (voir l'Annexe 5).
- **Interdiction de ré-identification** : la ré-identification délibérée des enregistrements dé-identifiés issus de comptes supprimés est interdite par une politique interne écrite. L'accès aux enregistrements résiduels (factures conservées, squelettes analytics) est restreint à un administrateur nommé unique, et les opérations admin sont consignées dans le journal d'audit. La rétention des journaux de 15 jours borne en outre la fenêtre pendant laquelle l'identifiant orphelin d'un compte supprimé reste joignable à une identité dans les journaux opérationnels.
- **Sécurité des postes de travail** : chiffrement intégral du disque (FileVault) et pare-feu logiciel activés sur tous les postes des fondateurs ; les réseaux domestiques des fondateurs utilisent WPA3.

6. Revue régulière

- Les mesures ci-dessus sont revues au regard d'un référentiel de contrôle RGPD interne (../rgpd/, structuré sur le guide sécurité de la CNIL), avec suivi du statut par item.

Annexe 3 : Suppression et restitution des données

Annexe au DPA Vook (art. 28(3)(g) RGPD). Décrit comment Vook (sous-traitant) restitue et/ou supprime les données à caractère personnel sur demande et en fin de contrat.

1. Périmètre

Données à caractère personnel traitées pour le compte du Responsable de traitement : données de compte, fichiers audio, transcriptions, synthèses et contenus de chat, ainsi que les métadonnées associées. Les données de facturation relèvent de règles de conservation légale distinctes (§5).

2. Restitution / export des données

- **Export en libre-service, pour une ou plusieurs transcriptions à la fois, tant que le compte est actif.** Les utilisateurs finaux exportent leurs propres contenus dans le produit, en plusieurs formats : transcriptions en PDF, DOCX, SRT, JSON, HTML et Markdown ; contenus de chat en PDF, DOCX et Markdown ; ainsi que le fichier audio d'origine. Le format JSON fournit une forme lisible par machine adaptée à la portabilité (art. 20).
- **API.** Les détenteurs de clé API exportent chaque transcription via GET /api/v1/transcriptions/:id/export (pdf, docx, html, md, srt).
- **Contrainte de chiffrement (par conception).** Le contenu est chiffré par utilisateur (§7) ; Vook ne peut pas le déchiffrer côté serveur, l'export est donc nécessairement réalisé par l'utilisateur, sous sa propre clé. Il n'existe aucune extraction de contenu en clair côté opérateur. C'est une propriété de confidentialité délibérée de la conception : même Vook ne peut pas lire le contenu d'un utilisateur. La restitution due au Responsable de traitement en fin de contrat est donc assurée par l'export en libre-service de ses utilisateurs, plutôt que par la remise de contenus déchiffrés par Vook.
- **Export global (feuille de route).** Un téléchargement en archive unique « exporter toutes mes données » figure sur la feuille de route. Le déchiffrement ayant lieu côté client sous la clé de l'utilisateur, cet export devra lui aussi être déclenché par l'utilisateur. Dans l'intervalle, l'export en libre-service décrit ci-dessus (une ou plusieurs transcriptions à la fois) est le mécanisme disponible et couvre déjà les droits des art. 15 et 20.

3. Suppression à la clôture du compte (mécanisme)

À la demande de suppression du compte (via l'application ou l'administration), Vook efface les données à caractère personnel de l'utilisateur dans tous les magasins de données, selon un principe uniforme : les enregistrements qui alimentent les analytics produit sont conservés mais réduits à un squelette analytique non personnel ; tout ce qui est personnel est détruit ou crypto-effacé. Concrètement :

1. **Annule l'abonnement Stripe actif et efface l'objet client Stripe** lorsque la loi le permet.
2. **Réduit les enregistrements de contenu à un squelette.** Transcriptions, synthèses, chat et métadonnées audio ne conservent que des champs non personnels (durées, compteurs, horodatages) ; noms, noms de fichiers, texte des transcriptions et contenus de chat sont mis à null.
3. **Procède au crypto-effacement** (destruction des clés de chiffrement) des clés par élément et par utilisateur, de sorte que tout texte chiffré restant (stockage, sauvegardes) devient définitivement illisible (§7).
4. **Supprime les objets de contenu stockés** (audio, transcriptions, diarisation, transcriptions mises en forme, chat) du stockage objet.
5. **Isole la facture conservée des données analytiques.** La facture, seul enregistrement conservé en clair (conservation légale comptable de 10 ans, §5), est rattachée à un enregistrement interne partagé « comptes supprimés » qui ne porte aucune donnée personnelle et n'apparaît sur aucun enregistrement analytique, tandis que chaque squelette analytique conservé garde l'identifiant d'origine, désormais orphelin et ne résolvant que vers des lignes non personnelles. Aucune clé stockée ne relie les deux, et la ré-identification délibérée est en outre interdite par une politique interne écrite (Annexe 2).
6. **Anonymise le compte.** Nom supprimé, email remplacé par un identifiant aléatoire ; un hachage à sens unique de l'adresse est conservé jusqu'à 12 mois, dans une liste autonome reliée à aucun enregistrement de compte, à seule fin d'empêcher la ré-inscription abusive d'un compte supprimé (intérêt légitime, prévention de la fraude), puis supprimé. Les identifiants d'authentification et le matériel de clés sont détruits et l'adresse de facturation supprimée.
7. **Supprime les événements analytiques de l'utilisateur (ClickHouse)** (§9) et révoque la session.

La suppression unitaire (une transcription, une synthèse ou un chat) applique le même effacement à la demande, à tout moment, tant que le compte est actif.

Suppression automatique des comptes inactifs.

Les comptes inactifs depuis plus de deux (2) ans sont supprimés automatiquement, après notification préalable de l'utilisateur et un délai de réponse de 30 jours, conformément à la politique de confidentialité de Vook. Cette suppression applique le même pipeline d'effacement que la clôture volontaire décrite ci-dessus.

4. Suppression à la fin du contrat

À la fin de la relation avec le Responsable de traitement, Vook supprime l'ensemble des données à caractère personnel des utilisateurs finaux du Responsable de traitement **sous 30 jours** à compter de la demande, sous la seule réserve de l'exception de conservation légale du §5 et de la fenêtre de rotation des sauvegardes du §6. La suppression est confirmée par écrit au Responsable de traitement et se propage aux sous-traitants ultérieurs (§8). Le contenu chiffré est rendu définitivement illisible par crypto-effacement (§7).

5. Exception de conservation légale

Les factures (contenant nom et adresse de facturation) sont conservées **10 ans** après la clôture du compte, comme l'exige le droit comptable français (Code de commerce, art. L123-22). Elles sont stockées dans le PostgreSQL de production et accessibles uniquement via le panneau d'administration (comptes nominatifs des fondateurs). Il s'agit d'une obligation légale qui prime sur les demandes de suppression pour ces documents précis.

6. Données résiduelles dans les sauvegardes

Les données d'un compte supprimé peuvent persister dans les sauvegardes PostgreSQL quotidiennes pendant la fenêtre de conservation de 30 jours au maximum, puis sont éliminées par rotation naturelle. Les sauvegardes ne sont pas modifiées enregistrement par enregistrement (pratique standard du secteur, pour éviter de corrompre les sauvegardes) ; l'anonymisation côté production est immédiate, ce qui rend les données résiduelles des sauvegardes difficiles à exploiter. L'accès aux sauvegardes est réservé à un administrateur nommé unique (identifiants Scaleway dédiés).

7. Fondement du crypto-effacement (contenu chiffré)

Le contenu utilisateur est stocké chiffré par utilisateur (AES-256). Le matériel de clés de chiffrement ne réside que dans la base de données applicative (il n'en existe aucune copie externe) ; la destruction des colonnes de clés à la suppression constitue donc l'effacement : le texte chiffré restant devient définitivement illisible, avec effet immédiat. C'est le fondement de l'effacement au sens du RGPD lorsqu'un objet ne peut pas être physiquement supprimé immédiatement. Sur le bucket de contenu Scaleway principal (Object Lock, mode COMPLIANCE), un objet supprimé est en outre purgé physiquement par le cycle de vie du stockage sous 90 jours ; sur les autres magasins (audio durable, magasin historique), l'effacement repose sur le seul crypto-effacement : les objets résiduels ne subsistent que sous forme de texte chiffré définitivement illisible, jusqu'à ce que le cycle de vie de chaque magasin les fasse expirer ou que le magasin soit retiré. Le même fondement couvre les résidus de sauvegarde de 30 jours (§6).

8. Suppression chez les sous-traitants ultérieurs

L'annulation de l'abonnement se propage à Stripe au moment de la suppression, et l'objet client Stripe est effacé lorsque la loi le permet. L'envoi d'emails (SendGrid) est utilisé comme simple relais SMTP : aucune liste de contacts ni enregistrement par utilisateur n'est stocké chez SendGrid, il n'y a donc rien à y supprimer ; l'exclusion des comptes supprimés de tout envoi est appliquée dans la propre base de données de Vook. Les enregistrements résiduels chez les autres sous-traitants ultérieurs sont couverts par le DPA de chaque sous-traitant ultérieur (voir l'Annexe 4).

9. Conservation des événements analytiques

Les événements analytiques comportementaux (qui portent des identifiants tels que des noms de fichiers, jamais de contenu) sont conservés au maximum **13 mois**, une limite appliquée nativement par un TTL au niveau de la table dans le magasin analytique, et non par procédure. Au-delà, ils ne subsistent que sous forme d'agrégats anonymes (des comptages sans identifiants), qui ne portent aucune donnée personnelle et sont conservés indéfiniment. Lors d'une suppression de compte, tous les événements analytiques de l'utilisateur sont supprimés purement et simplement du magasin analytique ; seuls demeurent les événements antérieurs à l'inscription rattachés à aucun compte. L'effacement atteint donc le magasin analytique comme le magasin principal.

Annexe 4 : Liste des sous-traitants ultérieurs

Annexe au présent Accord de traitement des données Vook (art. 28 RGPD). Vook agit en qualité de sous-traitant ; le Client est le responsable de traitement. La liste actuelle des sous-traitants ultérieurs autorisés, comprenant pour chacun : nom, rôle, données à caractère personnel traitées, entité juridique, lieu de traitement et base de transfert, est publiée et tenue à jour à l'adresse <https://vook.ai/fr/sub-processors>. Cette page fait partie intégrante de la présente Annexe 4 et est mise à jour conformément à l'article 4 du présent DPA. Les versions antérieures du présent DPA et de la liste des sous-traitants ultérieurs sont archivées selon la même convention de nommage (vook-dpa-fr-vAAAA-MM.pdf) afin que le Client puisse identifier la version en vigueur à une date donnée.

Annexe 5 : Analyse d'impact des transferts (TIA)

Annexe informative au DPA Vook. Documente l'évaluation par Vook du droit des pays tiers et des mesures supplémentaires pour chaque transfert de données personnelles hors UE/EEE (Schrems II / recommandations 01/2020 de l'EDPB ; clause 14 des CCT). Fournie à titre de transparence et pour aider le responsable de traitement dans sa propre évaluation. Cette annexe est une évaluation et non une garantie : elle reflète la situation à la date ci-dessous et est mise à jour avec la liste des sous-traitants ultérieurs (Annexe 4), selon le mécanisme de notification de l'article 4 du DPA.

1. Méthode

Selon la feuille de route en six étapes de l'EDPB : (1) les transferts sont cartographiés en Annexe 4 ; (2) l'outil de transfert est identifié pour chaque prestataire : module 3 des CCT, Data Privacy Framework (DPF) UE-États-Unis lorsque l'importateur est certifié, ou BCR (PayPal) ; (3) le droit du pays de destination est évalué ci-dessous (§2) ; (4) les mesures supplémentaires sont identifiées (§3) ; (5) les formalités contractuelles sont documentées dans le registre des DPA tenu par Vook ; (6) l'évaluation est réexaminée à chaque changement de sous-traitant ultérieur.

2. Droit du pays de destination évalué (États-Unis)

Tous les importateurs hors UE/EEE de l'Annexe 4 sont de droit américain. Le cadre juridique américain pertinent :

- **Article 702 du FISA** : permet l'acquisition ciblée des communications de personnes non américaines auprès des « fournisseurs de services de communications électroniques » américains.
- **CLOUD Act** : les sociétés de droit américain peuvent être contraintes de produire les données en leur possession, garde ou contrôle, quel que soit le lieu de stockage (c'est pourquoi une infrastructure située dans l'UE d'une société américaine ne supprime pas, à elle seule, l'exposition).
- **Data Privacy Framework (DPF) UE-États-Unis (décision d'adéquation de 2023)** : introduit des garanties contraignantes (limites de proportionnalité applicables au renseignement d'origine électromagnétique, la Data Protection Review Court (juridiction de révision)) ; lorsqu'un importateur est certifié DPF, la décision

d'adéquation fournit elle-même une base de transfert licite, les CCT étant conservées en solution de repli.

3. Mesures supplémentaires (les mesures déterminantes)

- **Chiffrement AES-256 par utilisateur du contenu au repos** : Vook chiffre les audios, transcriptions, résumés et conversations avant stockage, avec des clés par utilisateur que Vook ne peut pas utiliser pour déchiffrer côté serveur (sauf pour les utilisateurs ayant expressément activé l'option de clé de récupération, dont la clé est conservée enveloppée via Scaleway Key Manager). Une divulgation forcée du contenu stocké auprès de tout prestataire de stockage ou d'infrastructure ne produit que du texte chiffré ; les titres et noms de fichiers des transcriptions, stockés en clair comme métadonnées, font exception.
- **TLS 1.2+ en transit** sur tous les flux.
- **Résidence de traitement dans l'UE pour le stockage principal (Scaleway, Paris), l'inférence GPU (workers UE/EEE)** et les données d'observabilité au repos (Datadog EU1).
- **Traitement GPU éphémère** : aucun contenu conservé après un job ; sortie chiffrée avant renvoi.
- **Minimisation des données par prestataire** : chaque prestataire ne reçoit que les catégories listées en Annexe 4 ; le contenu n'atteint jamais les prestataires de paiement, d'e-mail, d'hébergement frontend, d'OAuth ou d'alerting.
- **Conditionnement au consentement** : le seul prestataire qui reçoit du contenu en clair (Google Gemini) le reçoit uniquement sur action explicite et consentie de l'utilisateur.

4. Évaluation par prestataire

RunPod, Inc. (workers UE/EEE)

- **Données transférées** : Contenu : texte chiffré au repos, en entrée comme en sortie ; en clair en mémoire GPU pendant l'inférence uniquement



- Outil : CCT (M3, DPA publié)
- Ce qu'une divulgation forcée US pourrait produire : Données stockées : texte chiffré. Une capture en mémoire nécessiterait l'interception prospective d'un job précis en cours d'exécution, un obstacle nettement plus élevé. Le modèle ne peut pas s'exécuter sur du texte chiffré : cette fenêtre est donc inhérente à la façon dont Vook réalise l'inférence aujourd'hui. Le matériel de calcul confidentiel (mode NVIDIA CC) y répond ; il est suivi, mais pas déployé.
- Risque résiduel : Faible à modéré, documenté

Google LLC (Gemini, point de terminaison global)

- Données transférées : Texte de transcription dans le prompt, uniquement sur action explicite et consentie de l'utilisateur ; offre payante, pas d'entraînement
- Outil : CCT (M3)
- Ce qu'une divulgation forcée US pourrait produire : Données de prompt/réponse conservées selon les conditions de l'offre payante de Google
- Risque résiduel : Modéré, en opt-in et documenté ; option de point de terminaison UE disponible (payante)

Stripe (branche US LLC)

- Données transférées : Données de paiement/facturation (pas de contenu)
- Outil : DPF + CCT
- Ce qu'une divulgation forcée US pourrait produire : Dossiers de paiement : données que Stripe détient de toute façon en tant que processeur PCI
- Risque résiduel : Faible

PayPal (maison mère US)

- Données transférées : Données de paiement (pas de contenu) ; responsable de traitement indépendant
- Outil : BCR
- Ce qu'une divulgation forcée US pourrait produire : Dossiers de paiement sous la responsabilité propre de PayPal
- Risque résiduel : Faible

Twilio SendGrid (traitement US)

- Données transférées : Adresse e-mail + contenu des e-mails (pas de transcriptions)
- Outil : CCT (M3)
- Ce qu'une divulgation forcée US pourrait produire : Trafic e-mail uniquement
- Risque résiduel : Faible

Vercel, Inc. (fonctions UE + Amérique du Nord)

- Données transférées : Métadonnées de compte/session/requête ; le contenu n'atteint jamais Vercel (traitement côté client)
- Outil : DPF + CCT
- Ce qu'une divulgation forcée US pourrait produire : Métadonnées uniquement
- Risque résiduel : Faible

Datadog, Inc. (EU1, données au repos en Allemagne)

- Données transférées : Logs techniques, métadonnées de requête ; rétention de 15 jours
- Outil : CCT (M3)
- Ce qu'une divulgation forcée US pourrait produire : Logs à courte durée de vie ; le support « follow-the-sun » peut accéder depuis l'extérieur de l'UE aux données stockées dans l'UE
- Risque résiduel : Faible

Google / Microsoft (OAuth)

- Données transférées : Identifiants de compte, e-mail, jeton OAuth
- Outil : CCT (M3)
- Ce qu'une divulgation forcée US pourrait produire : Identifiants de connexion que ces fournisseurs détiennent de toute façon en tant que fournisseurs d'identité grand public
- Risque résiduel : Faible

Slack (Salesforce, US)

- Données transférées : Contenus d'alertes internes ; données personnelles incidentes
- Outil : CCT (M3)
- Ce qu'une divulgation forcée US pourrait produire : Métadonnées incidentes
- Risque résiduel : Faible

5. Conclusion

Pour le cœur du service de transcription, le contenu de données personnelles est chiffré par utilisateur et résident dans l'UE : les scénarios réalistes de divulgation forcée visant des prestataires de droit américain produisent du texte chiffré ou des métadonnées périphériques, pas de contenu lisible. Les deux exceptions documentées sont le passage transitoire en clair en mémoire GPU pendant l'inférence (inhérent à la façon dont Vook réalise l'inférence aujourd'hui, localisé dans l'UE/EEE, éphémère) et la fonctionnalité IA en opt-in (action explicite et consentie de l'utilisateur, conditions d'offre payante sans entraînement, avec une option payante de point de terminaison UE). Vook évalue donc les mesures supplémentaires comme effectives pour les données et les transferts en jeu, tout en ne garantissant pas, conformément à l'article 6 du DPA, une exclusion totale de tout

traitement hors UE/EEE.

6. Réexamen

L'évaluation est réexaminée à chaque ajout ou remplacement d'un sous-traitant ultérieur (article 4 du DPA), en cas d'évolution significative du droit américain de la surveillance ou des orientations de la CJUE/EDPB, et au moins une fois par an.