Accord de traitement des données Vector

Projet contractuel conforme à la structure de l article 28 du RGPD

Version du 8 November 2026

Le présent accord encadre les traitements de données à caractère personnel effectués par VECTOR pour le compte d'un restaurant client. Il complète le contrat principal et doit être renseigné avec les faits de production signalés entre crochets avant signature. Il ne couvre pas les traitements pour lesquels VECTOR ou un prestataire détermine ses propres finalités et moyens en qualité de responsable du traitement distinct.

1 Parties et formation de l accord

1.1 Le responsable du traitement est le restaurant identifié dans le compte VECTOR, le bon de commande ou les conditions particulières, ci-après le « Responsable ».

1.2 Le sous-traitant est VECTOR SASU, société par actions simplifiée unipersonnelle au capital de 3 000 euros, dont le siège social est situé 62 boulevard Gambetta, 06000 Nice, France, immatriculée au RCS de Nice sous le numéro 130 982 390, SIREN 130 982 390, ci-après « VECTOR » ou le « Sous-traitant ». Contact vie privée : contact@vector-order.com.

1.3 Le présent accord, ses annexes et toute mise à jour valablement acceptée forment le « DPA ». Il constitue un acte juridique contraignant au sens de l'article 28, paragraphe 3, du règlement (UE) 2016/679 (« RGPD »).

1.4 Le DPA est conclu par signature ou par acceptation électronique par un utilisateur disposant des droits nécessaires pour engager le Responsable. En cas d'acceptation électronique, VECTOR conserve une preuve durable de cette acceptation, comprenant notamment l'identifiant du compte concerné, l'identité ou l'identifiant de l'utilisateur ayant procédé à l'acceptation, la date et l'heure de l'acceptation ainsi que la version du DPA acceptée.

2 Définitions et périmètre des rôles

2.1 Les termes « données à caractère personnel », « traitement », « violation de données à caractère personnel », « responsable du traitement », « sous-traitant », « autorité de contrôle » et « personne concernée » ont le sens du RGPD.

2.2 Le Responsable détermine les finalités et les moyens essentiels des traitements confiés. VECTOR agit comme sous-traitant pour les données de commandes, d'équipe, de support lié au compte du restaurant et, lorsqu'elles contiennent des données personnelles, les sources de menu traitées suivant les instructions du Responsable, dans les limites de l'Annexe I.

2.3 VECTOR demeure responsable du traitement pour ses finalités propres, notamment la gestion de sa relation commerciale, la facturation SaaS, la défense de ses droits, sa sécurité interne et ses obligations légales, dans la mesure où il détermine ces finalités et moyens. Ces traitements ne relèvent pas du présent DPA et doivent être décrits dans la politique de confidentialité applicable.

2.4 Stripe peut agir, selon le flux et ses conditions applicables, comme sous-traitant, sous-traitant ultérieur ou responsable du traitement indépendant. Les opérations dans lesquelles Stripe détermine ses propres finalités, notamment certaines obligations réglementaires, prévention de la fraude ou gestion de son réseau de paiement, sont exclues du mandat de sous-traitance de VECTOR. La qualification de chaque flux Stripe doit être vérifiée dans les contrats de production avant signature.

3 Objet durée nature et finalités

3.1 L'objet, la durée, la nature, les finalités, les catégories de personnes et les types de données sont décrits de façon détaillée à l'Annexe I. Le Responsable confirme que cette description est complète pour sa configuration du Service et informe VECTOR avant d'utiliser le Service pour un traitement non décrit.

3.2 Le traitement dure pendant le contrat principal, puis pendant la période de restitution et de suppression prévue à l'article 13. Les obligations qui, par leur nature, survivent à la fin du contrat restent applicables jusqu'à la suppression ou l'anonymisation irréversible des données confiées, sans préjudice des conservations imposées par la loi.

4 Instructions documentées et licéité

4.1 VECTOR ne traite les données confiées que sur instruction documentée du Responsable, y compris pour les transferts vers un pays tiers ou une organisation internationale. Constituent des instructions documentées : le présent DPA, le contrat principal, la configuration activée par le Responsable, les actions de ses utilisateurs autorisés et toute instruction écrite acceptée par VECTOR.

4.2 Si le droit de l'Union ou d'un État membre oblige VECTOR à traiter les données autrement, VECTOR en informe le Responsable avant le traitement, sauf si ce droit interdit cette information pour des motifs importants d'intérêt public.

4.3 VECTOR informe immédiatement le Responsable si, selon lui, une instruction enfreint le RGPD, une autre disposition du droit de l'Union ou le droit applicable d'un État membre en matière de protection des données. VECTOR peut suspendre l'instruction concernée pendant le temps raisonnablement nécessaire à sa clarification, sans modifier les autres traitements licites.

4.4 Le Responsable garantit qu'il dispose d'une base juridique, fournit les informations requises aux personnes concernées, respecte les principes de minimisation et d'exactitude, et n'introduit pas de données non nécessaires dans les notes libres ou les sources de menu. Il s'abstient de demander à VECTOR un traitement illicite.

5 Confidentialité et personnel autorisé

5.1 VECTOR veille à ce que les personnes autorisées à traiter les données s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée, reçoivent des accès limités à leurs fonctions et soient informées des règles de protection des données applicables.

5.2 VECTOR révoque ou adapte les accès lorsqu'ils ne sont plus nécessaires et encadre les accès administratifs ou de support. Le Responsable gère les rôles Owner, Manager et Staff de son établissement et retire sans délai les accès devenus inutiles.

6 Sécurité du traitement

6.1 Compte tenu de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, VECTOR met en œuvre et maintient les mesures techniques et organisationnelles appropriées décrites à l'Annexe II, conformément à l'article 32 du RGPD.

6.2 Ces mesures visent, selon les risques, la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes, la restauration de la disponibilité et l'évaluation régulière de l'efficacité des mesures. VECTOR peut faire évoluer les mesures sans diminuer substantiellement le niveau global de protection.

6.3 Toute mesure décrite comme « à confirmer » ou « à formaliser » à l'Annexe II n'est pas réputée mise en œuvre par la seule signature du DPA. VECTOR doit la vérifier, la corriger ou la supprimer avant signature. Le Responsable évalue si les mesures confirmées répondent aux risques de ses traitements.

7 Sous traitants ultérieurs

7.1 Le Responsable accorde une autorisation écrite générale à VECTOR pour recourir aux sous-traitants ultérieurs nécessaires au Service, sous réserve du présent article. La liste initiale est l'Annexe III. Un prestataire n'y figure que pour les traitements où sa qualité de sous-traitant ultérieur a été vérifiée.

7.2 VECTOR informe le Responsable par un moyen permettant une réception effective de tout projet d'ajout ou de remplacement au moins trente jours calendaires avant sa prise d'effet. La notification est adressée à l'Owner et au

contact contractuel enregistré par courriel et peut aussi être affichée dans le Service. La seule modification silencieuse d'une page publique ne vaut pas notification.

7.3 La notification indique au minimum l'identité du prestataire, les services concernés, les données et finalités, les lieux de traitement connus et, le cas échéant, le mécanisme de transfert. Le Responsable peut former, pendant le préavis, une objection écrite et motivée fondée sur la protection des données à contact@vector-order.com.

7.4 Les parties recherchent de bonne foi une solution raisonnable, notamment une mesure complémentaire, une configuration alternative ou la non-utilisation du nouveau prestataire pour le Responsable. Si aucune solution n'est raisonnablement possible avant la date prévue, le Responsable peut résilier sans pénalité le service matériellement affecté avant l'entrée en vigueur du changement. Les frais déjà dus pour une période commencée restent régis par le contrat principal, sous réserve du droit impératif.

7.5 VECTOR impose par contrat au sous-traitant ultérieur des obligations de protection des données substantiellement équivalentes à celles du présent DPA, notamment des garanties suffisantes et les obligations de l'article 28, paragraphe 3, dans la mesure applicable. VECTOR demeure pleinement responsable envers le Responsable de l'exécution par le sous-traitant ultérieur de ses obligations de protection des données.

7.6 En cas d'urgence liée à la sécurité ou à la continuité, VECTOR peut remplacer temporairement un prestataire avec un préavis plus court, à condition d'en informer le Responsable sans retard indu, d'expliquer l'urgence et de préserver le droit d'objection effectif.

8 Droits des personnes concernées

8.1 Compte tenu de la nature du traitement, VECTOR aide le Responsable, par des mesures techniques et organisationnelles appropriées, à s'acquitter de son obligation de répondre aux demandes d'exercice des droits prévus au chapitre III du RGPD, notamment l'accès, la rectification, l'effacement, la limitation, la portabilité, l'opposition et les droits relatifs aux décisions automatisées, dans la mesure où ils s'appliquent.

8.2 VECTOR transmet au Responsable sans retard indu toute demande reçue directement qui concerne manifestement un traitement confié. VECTOR ne répond pas au fond, sauf instruction documentée ou obligation légale, et peut vérifier raisonnablement l'identité du demandeur sans collecter de données excessives.

8.3 Le Responsable reste chargé de décider de la réponse et de respecter les délais légaux. VECTOR fournit les données ou fonctions raisonnablement disponibles et informe le Responsable si une demande ne peut être exécutée techniquement comme demandé.

9 Violations de données et incidents

9.1 VECTOR notifie au Responsable, sans retard injustifié après en avoir pris connaissance, toute violation de données à caractère personnel affectant les données confiées, conformément à l'article 33, paragraphe 2, du RGPD. La notification est adressée au contact désigné par le Responsable dans son compte VECTOR ou, à défaut, à l'adresse électronique associée au compte. Les incidents et violations de données peuvent être signalés à VECTOR à l'adresse suivante : contact@vector-order.com. VECTOR communique, dans la mesure où elles sont disponibles, les informations nécessaires permettant au Responsable de satisfaire à ses propres obligations de notification et complète ces informations progressivement lorsque celles-ci ne peuvent être fournies simultanément.

9.2 Dans la mesure des informations disponibles, la notification décrit : la nature de la violation ; les catégories et le nombre approximatif de personnes et d'enregistrements concernés ; le point de contact ; les conséquences probables ; et les mesures prises ou proposées pour remédier à la violation et en atténuer les effets. Les informations peuvent être communiquées par étapes sans retard indu.

9.3 VECTOR prend les mesures raisonnables pour contenir, analyser, corriger et documenter l'incident, conserve les éléments de preuve utiles et coopère avec le Responsable. VECTOR n'informe une autorité ou une personne concernée pour le compte du Responsable que sur instruction documentée, sauf obligation légale propre.

10 Assistance aux obligations des articles 32 à 36

10.1 Compte tenu de la nature du traitement et des informations dont il dispose, VECTOR aide le Responsable à assurer la sécurité prévue à l'article 32, à notifier les violations à l'autorité conformément à l'article 33, à communiquer aux personnes conformément à l'article 34, à réaliser les analyses d'impact prévues à l'article 35 et, le cas échéant, à préparer une consultation préalable au titre de l'article 36.

10.2 L'assistance peut inclure la description du Service et de ses mesures, les journaux pertinents, les informations sur les sous-traitants ultérieurs, les éléments factuels relatifs à un incident et les réponses raisonnables aux questions d'une autorité. VECTOR ne remplace pas le Responsable dans ses décisions ni dans son analyse de licéité.

11 Transferts internationaux

11.1 VECTOR et ses sous-traitants ultérieurs ne transfèrent ni ne rendent accessibles les données confiées hors de l'Espace économique européen, sauf instruction documentée du Responsable et respect du chapitre V du RGPD.

11.2 Tout transfert repose sur une décision d'adéquation applicable ou, à défaut, sur des garanties appropriées, telles que les clauses contractuelles types de la décision d'exécution (UE) 2021/914 dans le module pertinent, accompagnées d'une évaluation du transfert et de mesures supplémentaires lorsque nécessaire. Les dérogations de l'article 49 ne sont utilisées qu'à titre exceptionnel et documenté.

11.3 VECTOR fournit, sur demande, les informations raisonnablement nécessaires sur le mécanisme, le pays de destination et les mesures complémentaires, sous réserve de la sécurité et de la confidentialité. VECTOR informe le Responsable si le mécanisme cesse d'être valable et suspend ou adapte le transfert si aucune solution conforme n'est disponible.

11.4 Les clauses de la décision (UE) 2021/915 encadrent la relation responsable-sous-traitant au titre de l'article 28 ; elles ne constituent pas, à elles seules, un mécanisme de transfert du chapitre V. Le présent DPA s'inspire de leur structure sans déclarer leur incorporation intégrale ni leur signature autonome.

12 Informations démonstration et audits

12.1 VECTOR met à la disposition du Responsable toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 et contribue aux audits, y compris aux inspections, menés par le Responsable ou un auditeur indépendant mandaté par lui.

12.2 Sauf incident, demande d'une autorité ou indice sérieux de non-conformité, le Responsable donne un préavis raisonnable d'au moins quinze jours ouvrés, limite l'audit à une fois par période de douze mois et privilégie d'abord les documents, questionnaires, rapports ou certifications disponibles. Ces limites ne restreignent pas les droits impératifs du Responsable ou de l'autorité de contrôle.

12.3 L'audit se déroule pendant les heures ouvrées, avec une perturbation minimale, sous confidentialité et sans accès aux données d'autres clients, aux secrets d'affaires non pertinents ni aux vulnérabilités exploitables. L'auditeur ne doit pas être un concurrent direct de VECTOR et doit présenter des garanties de compétence et de confidentialité ; VECTOR ne peut imposer unilatéralement son propre auditeur.

12.4 Chaque partie supporte ses coûts ordinaires. Les prestations extraordinaires demandées au-delà des informations standard peuvent être facturées à un coût raisonnable convenu à l'avance, sauf si l'audit révèle une violation substantielle imputable à VECTOR ou découle d'un incident confirmé imputable à VECTOR.

12.5 VECTOR corrige sans retard indu toute non-conformité avérée relevant de sa responsabilité et informe le Responsable des mesures prises. Une autorité de contrôle conserve l'ensemble de ses pouvoirs.

13 Restitution suppression et fin du traitement

13.1 À la fin du contrat, le Responsable dispose pendant quatre-vingt-dix jours d'un accès en lecture seule à son compte et peut demander l'export des données disponibles relevant de son traitement. VECTOR met à disposition, sur demande raisonnable, un export de ces données dans un format techniquement exploitable et couramment utilisé.

13.2 Au choix du Responsable communiqué avant l'expiration de cette période, VECTOR restitue les données puis supprime les copies, ou les supprime directement, sauf si le droit de l'Union ou d'un État membre exige leur conservation. À défaut de choix reçu, VECTOR les supprime ou les anonymise après la période de quatre-vingt-dix jours, sous réserve des conservations légales distinctes.

13.3 Les données conservées pour une obligation légale sont isolées, protégées, rendues inaccessibles aux usages ordinaires et traitées uniquement pour cette obligation jusqu'à leur échéance. Une conservation poursuivie pour les finalités propres de VECTOR relève de sa qualité de responsable du traitement et doit disposer d'une base légale distincte.

13.4 Les éventuelles copies résiduelles présentes dans les sauvegardes sont supprimées conformément au cycle normal de rotation et de purge des sauvegardes de VECTOR. Elles restent protégées, ne sont pas utilisées à des fins opérationnelles et ne sont restaurées qu'en cas de nécessité de continuité ou de reprise. Toute donnée restaurée reste soumise aux obligations de suppression applicables.

13.5 Les fichiers source transmis dans le cadre de la fonctionnalité AI Menu Import sont programmés pour suppression par VECTOR environ trente jours après leur dépôt. Lorsque le traitement implique un sous-traitant ultérieur, les conditions de conservation applicables par ce sous-traitant sont celles décrites dans la documentation contractuelle et la liste des sous-traitants ultérieurs de VECTOR. Les brouillons, journaux et états de crédit obéissent aux durées distinctes définies à l'Annexe I.

13.6 Sur demande raisonnable, VECTOR confirme par écrit l'achèvement de la suppression relevant de son contrôle, sous réserve des sauvegardes résiduelles et des conservations légales identifiées.

14 Demandes des autorités et divulgations obligatoires

14.1 Sauf interdiction légale, VECTOR informe le Responsable de toute demande contraignante d'une autorité portant sur les données confiées, vérifie la validité de la demande, limite la divulgation à ce qui est légalement requis et documente sa réponse.

14.2 Lorsque la demande émane d'un pays tiers, VECTOR évalue les exigences du chapitre V et les garanties applicables. Il conteste une demande manifestement illicite lorsqu'il existe des motifs raisonnables et des voies effectives, dans la mesure permise par le droit applicable.

15 Non conformité suspension et résiliation

15.1 Si VECTOR ne respecte pas le DPA, le Responsable peut demander la suspension du traitement concerné jusqu'au rétablissement de la conformité. VECTOR informe promptement le Responsable s'il n'est plus en mesure de respecter ses obligations.

15.2 Le Responsable peut résilier le service affecté si la conformité n'est pas rétablie dans un délai raisonnable, si VECTOR viole substantiellement ou de manière persistante le DPA, ou si une décision contraignante constate une violation. VECTOR peut résilier le traitement si le Responsable maintient une instruction illicite après avoir été averti.

15.3 La fin du DPA déclenche l'article 13. Elle ne prive aucune partie des droits et recours prévus par le RGPD ou le droit impératif.

16 Responsabilité et coûts d assistance

16.1 La responsabilité des parties au titre du RGPD est régie par ses articles 79 à 82 et le droit applicable. Aucune clause du contrat principal ne limite les droits d'une personne concernée ou les pouvoirs d'une autorité, ni une responsabilité qui ne peut légalement être limitée.

16.2 Entre les parties, les limitations du contrat principal s'appliquent dans la mesure permise par le droit et sans neutraliser les obligations essentielles du présent DPA.

16.3 L'assistance standard requise par les articles 8 à 12 est comprise dans le Service. Les demandes manifestement excessives ou nécessitant un développement spécifique peuvent faire l'objet d'un devis préalable raisonnable, sans empêcher l'exécution d'une obligation légale urgente.

17 Hiérarchie modification et dispositions finales

17.1 En cas de contradiction relative aux traitements confiés, l'ordre de priorité est : les clauses impératives du RGPD ; les clauses contractuelles types valablement conclues pour un transfert au titre du chapitre V ; le présent DPA et ses annexes ; les conditions particulières ; puis le contrat principal. Une clause ajoutée ne peut contredire directement ou indirectement les clauses types applicables ni porter atteinte aux droits fondamentaux.

17.2 Une modification matérielle du DPA requiert une notification effective et, lorsqu'elle modifie les obligations essentielles ou les instructions, une nouvelle acceptation ou un avenant. Une mise à jour factuelle de la liste des sous-traitants suit l'article 7. Une modification imposée par le droit peut prendre effet au moment nécessaire, avec information du Responsable.

17.3 Si une clause est invalide, les autres restent applicables. Les parties remplacent la clause par une disposition valide se rapprochant de son objet tout en préservant les exigences du RGPD.

17.4 Le droit et le tribunal prévus au contrat principal s'appliquent entre les parties, sans préjudice des droits des personnes concernées, des règles de compétence du RGPD et des pouvoirs de l'autorité de contrôle.

Annexe I Description des traitements confiés

Cette annexe constitue la description exigée par l'article 28, paragraphe 3. Elle doit correspondre aux modules réellement activés pour le Responsable.

A Objet durée nature et finalités

Champ	Description
Objet	Fourniture d'un SaaS de carte numérique, QR, prise et gestion de commandes, comptes d'équipe, support et, selon l'offre, fonctions de paiement, caisse, documents et statistiques.
Durée	Durée du contrat, période de lecture seule et d'export de 90 jours, puis suppression ou anonymisation, sous réserve des conservations légales et du cycle de sauvegarde à confirmer.
Nature	Collecte, enregistrement, structuration, hébergement, consultation autorisée, transmission, rapprochement, journalisation, sauvegarde, export, limitation, suppression et anonymisation. Pour AI Menu Import : stockage temporaire, extraction automatisée, retour d'un brouillon et revue humaine.
Finalités	Exécuter les instructions du restaurant : administrer les utilisateurs ; afficher les menus et QR ; transmettre, préparer, suivre et documenter les commandes ; assister les utilisateurs ; sécuriser le Service ; fournir les fonctions activées ; restituer ou supprimer les données.
Fréquence	Traitement continu pendant l'utilisation du Service, avec traitements ponctuels pour le support, l'export et AI Menu Import.

B Personnes données et opérations

Personnes	Données confiées	Opérations et finalités
Clients du restaurant	Table ou QR, articles, quantités, options, notes, horaires, retrait, identifiant ou adresse électronique de document si fournie, références de paiement limitées.	Collecter, transmettre, suivre, rembourser lorsque autorisé, documenter et fournir les justificatifs.
Équipe du restaurant	Nom, adresse électronique, rôle, permissions, invitations, identifiants de compte, événements d'authentification et journaux.	Créer les comptes, authentifier, contrôler les accès, assurer la sécurité et la traçabilité.
Contacts professionnels	Coordonnées, contenu des demandes et échanges de support.	Recevoir, traiter, suivre et conserver les demandes liées au Service.
Personnes figurant dans une source de menu	Photos ou PDF fournis par le restaurant, contenu extrait, brouillon, décisions de revue et métadonnées techniques.	Stockage temporaire, transfert technique au service d'extraction, génération d'un brouillon et validation humaine.

C Catégories particulières et données à risque

Aucune catégorie particulière de données au sens de l'article 9 ni donnée pénale au sens de l'article 10 n'est requise par défaut. Les notes libres et documents peuvent toutefois contenir des informations imprévues. Le Responsable doit interdire ou minimiser leur saisie. Si un traitement régulier de données sensibles devient nécessaire, les parties mettent à jour cette annexe, documentent la base juridique et renforcent les mesures avant activation.

D Durées et sort des données

Catégorie	Règle contractuelle	Fait à confirmer avant signature
Données opérationnelles confiées	Relation active puis 90 jours en lecture seule et export ; suppression ou anonymisation ensuite, sauf conservation légale distincte.	Périmètre et formats d'export ; délais de purge des systèmes actifs.
Sources AI Menu Import	Suppression programmée environ 30 jours après dépôt.	Exécution du nettoyage ; conservation côté Gemini ; sort des copies et erreurs.
Brouillons AI métadonnées et crédits	Règle distincte de celle des fichiers source.	Durées exactes et base de conservation.
Journaux de sécurité et support	Conservation limitée aux besoins de sécurité, preuve et assistance.	Durées exactes, accès et procédure de purge.
Sauvegardes	Purge selon cycle normal, protection et absence d'usage ordinaire.	Durée maximale, fréquence, tests et procédure de suppression après restauration.
Données fiscales comptables ou de preuve	Conservation uniquement si une obligation légale ou un motif propre documenté l'exige.	Données concernées, durée, qualité de responsable ou sous-traitant et contrôle d'accès.

E Obligations et droits du Responsable

Le Responsable donne les instructions, choisit les modules et paramètres, gère ses utilisateurs, informe les personnes, définit les bases juridiques et durées qui lui incombent, répond aux demandes de droits, évalue les risques et contrôle les garanties de VECTOR. Il peut demander les informations, l'assistance et les audits prévus au DPA.

Annexe II Mesures techniques et organisationnelles

Les mesures ci-dessous reprennent les contrôles documentés dans les sources VECTOR. Les éléments non prouvés restent signalés. La signature ne transforme pas un contrôle à confirmer en contrôle existant.

Domaine	Mesures décrites	Statut de production
Gouvernance	Responsabilités de sécurité, confidentialité du personnel, revue des risques, procédures et registre des activités de sous-traitance.	Confidentialité annoncée ; politiques, responsables, registre et fréquence de revue à confirmer.
Séparation des clients	Isolation logique par restaurant et contrôles côté serveur tenant compte du rôle et de l'établissement.	Décrit dans les documents ; tests d'isolation et revue périodique à confirmer.
Identités et accès	Comptes personnels, rôles Owner Manager Staff, principe du besoin d'en connaître, retrait des accès, protection des sessions et jetons à usage limité.	Contrôles décrits ; MFA administrateur, cycle de revue et procédure de départ à confirmer.
Authentification	Mots de passe hachés et mécanismes d'authentification protégés.	Algorithme, paramètres, politique de mot de passe et protection contre les tentatives à confirmer.
Chiffrement	TLS en transit fourni par l'infrastructure ; secrets tenus hors du client.	Versions TLS, chiffrement au repos, gestion et rotation des clés à confirmer.
Journalisation	Journaux pour opérations sensibles, sécurité, diagnostic et mécanismes d'intégrité fiscale.	Événements, durée, protection, alertes et accès aux journaux à confirmer.
Sécurité applicative	Gestion des dépendances, séparation des environnements et limitation des secrets.	Processus de correctifs, revues de code, tests, scans et délais de remédiation à formaliser.
Disponibilité et reprise	Sauvegarde et restauration prévues ; procédures d'incident.	Architecture, fréquence, rétention, RPO RTO, tests de restauration et continuité à confirmer.
Gestion des incidents	Détection, analyse, confinement, correction, documentation et notification au Responsable.	Plan, astreinte, canal d'urgence, exercices et objectif de notification à confirmer.
Sous-traitants	Évaluation des garanties, contrats avec obligations équivalentes, suivi des changements.	DPA, entités, pays, sous-traitants et transferts à vérifier pour chaque prestataire.
Minimisation et suppression	Limitation des accès et des données ; fichiers source AI programmés pour suppression vers 30 jours ; suppression après fin du contrat.	Preuves de tâches de purge, durées des autres catégories et cycle des sauvegardes à confirmer.
Évaluation de l'efficacité	Tests et revues réguliers des mesures de sécurité adaptés aux risques.	Programme, périodicité, propriétaires et conservation des résultats à formaliser.

Annexe III Sous traitants ultérieurs et rôles distincts

Cette liste ne vaut autorisation que pour les rôles et traitements vérifiés. Les mentions entre crochets doivent être renseignées à partir des contrats et comptes de production.

Prestataire	Service et données	Qualification	Entité lieux et transferts
Cloudflare	Workers, D1, R2, réseau et sécurité ; comptes, restaurant, commandes, journaux, actifs, sources AI et archives selon configuration.	Sous-traitant ultérieur pour les traitements hébergés, sous réserve du DPA de production.	Entité contractante, régions, sous-traitants, lieux d'accès, DPA, mécanisme du chapitre V et mesures complémentaires.]
Resend	Courriels transactionnels ; destinataire, langue, objet, contenu, état et identifiant du message.	Sous-traitant ultérieur, sous réserve du DPA et du compte de production.	Entité, hébergement, sous-traitants, DPA, transferts et conservation.]
Google Gemini	Extraction de menus ; fichier fourni, instruction technique, sortie et métadonnées d'usage. Aucune commande, paiement ou archive fiscale dans le flux documenté.	Sous-traitant ultérieur uniquement si le compte et les conditions de production applicables le confirment.	Offre API payante appropriée, entité, DPA, conservation, lieux, transferts et usage des données.]
Stripe	Facturation SaaS, achat ponctuel, Stripe Connect, paiement, remboursement et références limitées.	Qualification variable : sous-traitant, sous-traitant ultérieur ou responsable distinct selon le flux. Les flux où Stripe agit comme responsable distinct ne relèvent pas de l'autorisation de sous-traitance.	Entité contractante, conditions Connect, DPA, responsabilités, pays, mécanismes et mesures.]

Procédure de changement Notification effective au moins trente jours à l'avance par courriel aux contacts enregistrés, informations suffisantes, objection motivée, recherche d'une solution et droit de résiliation du service affecté selon l'article 7.

Références juridiques de rédaction

Règlement (UE) 2016/679, notamment articles 28 paragraphes 2 à 4 et 9, 32 à 36 et chapitre V. Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre responsables du traitement et sous-traitants. Décision d'exécution (UE) 2021/914 pour les clauses contractuelles types applicables à certains transferts internationaux. Guide du sous-traitant de la CNIL. Ces références servent à la rédaction et ne remplacent pas l'examen des faits, contrats fournisseurs et mesures réellement déployées.