Souveraineté des données.

Version 1.0 · en vigueur le 15 novembre 2026

1. Objet et portée

1.1. Ce que couvre cette page. Elle dit où sont hébergées les données que vous nous confiez, chez quels fournisseurs, sous quel droit, ce que changent les lois extraterritoriales, et quelles options nous recommandons selon l'usage, intelligence artificielle comprise.

1.2. À qui elle s'applique. Aux clients de BONBAY et de ses quatre marques, pour les données que nous hébergeons, sauvegardons ou traitons pour eux. Elle intéresse en particulier les DSI, les acheteurs et les entreprises soumises à la directive NIS 2 ou à un secret professionnel.

1.3. Articulation. Les engagements contractuels figurent à l'article 13.5 et dans l'annexe D des CGV ; les transferts hors de l'Union sont traités à la section 9 de notre politique de données personnelles. La liste nominative des prestataires est sur la page Sous-traitants ultérieurs ; cette page explique les choix qui la fondent.

2. Où sont vos données par défaut

CE QUI EST HÉBERGÉ	CHEZ QUI	OÙ
Sites, applications et bases de données que nous hébergeons pour vous	OVHcloud ; sites produits avec notre partenaire Thrive	France (Roubaix, Gravelines)
Sauvegardes quotidiennes chiffrées, conservées 30 jours	Scaleway, second fournisseur, autre région	France (Paris)
Messagerie et documents de BONBAY	OVHcloud	France
Gestion interne : suivi commercial Pilote, coffre d'accès, documents	Nexus	Union européenne
Banque et facturation	Qonto	Union européenne
Paiements en ligne	Stripe	Union européenne, une partie des traitements aux États-Unis, encadrée (politique de données, section 9)

Deux fournisseurs différents pour la production et les sauvegardes : une panne, un litige ou la fermeture d'un compte chez l'un ne fait pas disparaître vos données chez l'autre. Nos objectifs de reprise sont sur la page Continuité et réversibilité.

---

3. Les questions à ne pas confondre

3.1. Où sont les serveurs ? C'est la localisation : le pays et le centre de données où les données sont stockées et traitées.

3.2. Qui contrôle le fournisseur ? C'est le droit auquel sont soumises la société qui exploite les serveurs et sa maison mère. Un centre de données à Paris peut appartenir à une société dont la maison mère est américaine.

3.3. Qui peut y accéder, et d'où ? C'est l'accès : support technique, administration à distance, sous-traitants du fournisseur. Un accès depuis un pays tiers à des données stockées en Europe est un transfert au sens du chapitre V du RGPD.

Nous parlons de données souveraines quand les trois réponses mènent à l'Union européenne. L'article 13.5 de nos CGV le rappelle : une région d'hébergement annoncée ne suffit pas, à elle seule, à établir qu'aucun transfert ou accès depuis un pays tiers n'a lieu.

---

4. Les lois extraterritoriales

4.1. Le Cloud Act américain. Adopté en 2018, le Clarifying Lawful Overseas Use of Data Act permet aux autorités américaines, dans une enquête pénale et selon les procédures du droit américain (mandat, injonction), d'exiger d'un fournisseur soumis à ce droit les données qu'il a en sa possession, sous sa garde ou sous son contrôle, même stockées hors des États-Unis. Le fournisseur peut contester la demande dans des cas limités. Il peut se voir interdire d'en prévenir son client.

4.2. Le renseignement. Le droit américain du renseignement permet aussi aux services d'obtenir des fournisseurs des données de personnes non américaines situées à l'étranger. La Cour de justice de l'Union européenne l'a examiné, notamment la section 702 du FISA, dans l'arrêt Schrems II du 16 juillet 2020 (affaire C-311/18), qui a invalidé le Privacy Shield.

4.3. Le cadre UE-États-Unis. Depuis la décision d'adéquation du 10 juillet 2023 (décision d'exécution (UE) 2023/1795), un transfert vers une entreprise américaine certifiée au cadre de protection des données UE-États-Unis est licite sans autre formalité. Ce cadre encadre le transfert ; il ne supprime pas les accès prévus par le droit américain. Ses deux prédécesseurs, Safe Harbor en 2015 puis Privacy Shield en 2020, ont été invalidés par la Cour de justice.

4.4. Ce que dit le droit européen et français. L'article 48 du RGPD prévoit qu'une décision d'une juridiction ou d'une autorité d'un pays tiers exigeant un transfert n'est reconnue que si elle se fonde sur un accord international, comme un traité d'entraide judiciaire. L'article 32 du règlement (UE) 2023/2854 sur les données impose aux fournisseurs de services en nuage des mesures contre un accès gouvernemental étranger aux données non personnelles contraire au droit de l'Union. La loi n° 68-678 du 26 juillet 1968, dite loi de blocage, encadre la communication de certaines informations économiques à des autorités étrangères. Ces textes créent un conflit de lois ; ils n'empêchent pas un fournisseur américain d'être contraint par son propre droit.

4.5. Et BONBAY ? BONBAY est une SAS française, sans maison mère hors de l'Union européenne. Si une autorité étrangère nous demandait vos données, nous ne répondrions que dans le cadre d'un accord international (article 48 du RGPD), nous vous préviendrions sauf interdiction légale, et nous contesterions une demande sans fondement. Un fournisseur français reste soumis au droit français : réquisitions judiciaires, techniques de renseignement du Code de la sécurité intérieure. La souveraineté ne signifie pas qu'aucune autorité ne peut accéder aux données, mais que l'accès suit le droit européen et français, avec ses garanties et ses recours.

5. Ce que change un hébergement en Europe chez un fournisseur américain

CE QUI CHANGE	CE QUI NE CHANGE PAS
Les données sont stockées et traitées dans l'Union, sous le RGPD	La maison mère reste soumise au Cloud Act et au droit américain du renseignement
Les données ne sont pas stockées aux États-Unis	Le support, l'administration à distance ou un sous-traitant situé hors de l'Union peuvent constituer un transfert
Certaines offres permettent de garder les clés de chiffrement chez vous	Si le fournisseur détient les clés, il peut être contraint de remettre les données en clair
L'engagement de localisation est opposable au fournisseur	Un engagement contractuel ne l'emporte pas sur une loi à laquelle le fournisseur est soumis

La mesure la plus efficace, selon les recommandations 01/2020 du Comité européen de la protection des données, est un chiffrement fort dont les clés restent hors de portée du fournisseur. Nos sauvegardes sont chiffrées avant d'être envoyées, avec des clés gardées par BONBAY. Pour un besoin réglementaire, nous orientons vers une offre qualifiée SecNumCloud par l'ANSSI : la version 3.2 de ce référentiel exige notamment que le fournisseur soit protégé des lois extra-européennes. La liste des offres qualifiées est publiée sur cyber.gouv.fr.

6. Options recommandées par usage

Pour chaque usage, l'option que nous recommandons par défaut et l'endroit où vont les données. Vous pouvez en choisir une autre : nous vous disons ce que cela change, au devis.

USAGE	OPTION RECOMMANDÉE	OÙ SONT LES DONNÉES
Site vitrine, boutique, application métier et sa base	Hébergement OVHcloud souscrit par BONBAY	France (Roubaix, Gravelines)
Sauvegardes	Scaleway, chiffrement avant envoi, clés chez BONBAY	France (Paris), chez un second fournisseur
Assistant d'IA sur des documents internes sensibles, sans données personnelles	Mistral AI par API, offre professionnelle sans entraînement	Union européenne, fournisseur français
Données personnelles réelles, données soumises à un secret professionnel, ou exigence qu'aucune donnée ne quitte des serveurs que nous maîtrisons	IA hébergée en France : modèle à poids ouverts sur des serveurs OVHcloud ou Scaleway, sur votre instruction écrite	France, aucun envoi à un fournisseur d'IA tiers
Rédaction, code, analyse de contenus publics ou pseudonymisés	Anthropic (Claude), OpenAI ou Google (Gemini) selon la tâche, en région européenne quand l'offre le permet	Union européenne ou États-Unis selon l'offre ; transfert encadré et inscrit dans l'annexe D
Échanges et documents avec notre équipe	Messagerie et documents OVHcloud de BONBAY	France
Données de santé, entité soumise à NIS 2, exigence d'un marché public	Hébergeur certifié HDS ou offre qualifiée SecNumCloud, choisi avec vous	France, chez un fournisseur dont la qualification couvre le service utilisé

7. L'intelligence artificielle et la souveraineté

7.1. Deux options souveraines. Mistral AI, fournisseur français, est notre option par défaut pour les données sensibles, par son API professionnelle sans entraînement. L'IA hébergée en France va plus loin : un modèle à poids ouverts tourne sur des serveurs OVHcloud ou Scaleway en France, et aucune requête ne part vers un fournisseur tiers.

7.2. Les fournisseurs américains. Anthropic, OpenAI et Google proposent des modèles parfois plus performants pour le code ou l'analyse. Nous les utilisons en offre professionnelle ou par API, sans entraînement sur les données transmises, en région européenne quand l'offre le permet. Ils ne reçoivent pas de données personnelles, sauf instruction écrite de votre part ; les contenus sont pseudonymisés avant envoi, et la table de correspondance reste chez nous ou chez vous.

7.3. Le prix de la souveraineté. Un modèle hébergé en France demande des serveurs dédiés : son coût fixe est plus élevé pour de faibles volumes, et sa qualité peut être inférieure sur certaines tâches. Nous le chiffrons au devis à côté de l'option par API, pour que vous choisissiez en connaissance de cause. Le budget des usages est encadré selon Maîtrise des tokens ; ce qui part vers un modèle est détaillé dans IA et vos données.

---

8. Ce que vous choisissez

Le niveau d'exigence. Au devis, vous indiquez si vos données doivent rester en France, dans l'Union européenne, ou chez des fournisseurs sans maison mère hors de l'Union. Nous ne retenons alors que les options compatibles.
Les fournisseurs d'IA. Vous pouvez exclure tout fournisseur non européen : il n'est pas inscrit dans votre annexe D, et nous travaillons avec Mistral AI ou l'IA hébergée en France.
Le titulaire des comptes. Hébergement et clés d'API peuvent être ouverts à votre nom : vous gardez la relation contractuelle avec le fournisseur et la main sur les accès.
Les changements. Un changement de prestataire ou de lieu de traitement vous est annoncé 30 jours avant, avec un droit d'opposition (Sous-traitants ultérieurs).
La sortie. Vos données, contenus et code vous sont remis dans des formats ouverts sous 15 jours ouvrés après votre demande : vous pouvez changer d'hébergeur sans dépendre de nous.

Votre choix est écrit dans l'annexe D, avec les lieux d'hébergement, les accès et les transferts éventuels.

---

9. Limites

Aucune qualification revendiquée. BONBAY n'est ni certifiée HDS ni qualifiée SecNumCloud. Quand ces titres sont exigés, ils doivent être détenus par le fournisseur retenu, et nous vérifions qu'ils couvrent le service réellement utilisé.
Un fournisseur européen n'est pas hors d'atteinte. Une filiale ou une activité aux États-Unis peut l'exposer à des demandes, et le droit français prévoit ses propres accès. Nous vérifions la structure de contrôle de chaque fournisseur à son entrée et à la revue annuelle.
Les outils que vous choisissez. Votre messagerie, votre suite bureautique ou votre logiciel de gestion relèvent de vos contrats. Bonbay Cyber peut évaluer leur exposition dans une mission dédiée.
Le cadre UE-États-Unis peut tomber. S'il était invalidé, nous vous en informerions sans délai et proposerions des clauses contractuelles types avec mesures complémentaires, ou une option européenne.

Le transport. Sur Internet, des données chiffrées en transit (TLS 1.2 au moins) peuvent traverser des réseaux hors de l'Union : le chiffrement les protège, le trajet ne se contrôle pas.

10. Contact et mise à jour

10.1. Responsable. Pierre Marsanne, président de BONBAY, porte la sécurité, la confidentialité et la protection des données. Question sur un lieu d'hébergement, demande d'option souveraine : contact@bonbay.fr, ou BONBAY, 38 cours de l'Intendance, 33000 Bordeaux. Une faille se signale à la même adresse, reprise dans https://www.bonbay.fr/.well-known/security.txt.

10.2. Version. Version 1.0, en vigueur le 15 novembre 2026. Cette page est revue chaque année (prochaine revue : novembre 2027) et à chaque changement important, de nos fournisseurs comme de la loi. Vous êtes prévenu par e-mail d'un changement qui vous concerne. Nos autres engagements sont réunis dans le Centre de confiance.

10.3. Textes. RGPD : règlement (UE) 2016/679. Règlement sur les données : règlement (UE) 2023/2854. Transferts hors de l'Union : cnil.fr.