RGPD et sous-traitance.

Version 1.0 · en vigueur le 15 novembre 2026

1. Objet et portée

1.1. Ce que couvre cette page. Elle décrit nos obligations lorsque BONBAY traite des données personnelles pour votre compte et sur vos instructions : les données de vos clients, prospects, salariés, adhérents ou usagers. Cela arrive dans les missions de nos quatre marques : hébergement ou maintenance d'un site, intégration d'un assistant d'IA, audit de sécurité sur vos systèmes, migration d'une base, formation sur vos documents réels.

1.2. À qui elle s'applique. À tout client professionnel de BONBAY, SAS au capital de 4 500 €, 38 cours de l'Intendance, 33000 Bordeaux, dès qu'une mission touche des données personnelles dont il est responsable.

1.3. Articulation avec nos documents. Le cadre contractuel est fixé par l'article 13 des conditions générales de vente et par leur annexe D, l'accord de traitement des données. Les traitements que nous menons pour nous-mêmes (site, prospects, facturation, stagiaires) sont décrits dans notre politique de données personnelles. Cette page peut être annexée à votre devis : elle ajoute des engagements à l'annexe D sans en retirer aucun. Quand elle fixe un délai plus favorable pour vous que l'annexe D, c'est ce délai que nous appliquons.

2. Qui est responsable de quoi

2.1. Deux rôles. Le responsable de traitement décide pourquoi et comment des données sont traitées (article 4.7 du RGPD). Le sous-traitant les traite pour son compte et sur ses instructions (article 4.8). Le rôle se détermine traitement par traitement, d'après ce que chacun décide réellement, et non d'après l'intitulé du devis (article 13.1 des CGV).

SITUATION	RÔLE DE BONBAY	QUI RÉPOND AUX PERSONNES CONCERNÉES
Vous nous écrivez, demandez un devis, êtes client ou stagiaire de Bonbay Académie	Responsable de traitement	BONBAY
Nous hébergeons ou maintenons votre site et sa base de clients	Sous-traitante (article 28)	Vous, avec notre aide

SITUATION	RÔLE DE BONBAY	QUI RÉPOND AUX PERSONNES CONCERNÉES
Nous intégrons un assistant d'IA qui lit les demandes de vos clients	Sous-traitante (article 28)	Vous, avec notre aide
Nous auditons vos systèmes et voyons les comptes de vos salariés	Sous-traitante (article 28)	Vous, avec notre aide
Vous et nous décidons ensemble des finalités d'un traitement	Responsable conjoint (article 26)	Selon l'accord écrit conclu avant le traitement

2.2. Pas de changement de rôle en silence. Un sous-traitant qui déciderait lui-même des finalités d'un traitement en deviendrait responsable (article 28.10 du RGPD). Nous ne le faisons pas : vos données ne servent qu'à la mission que vous avez commandée.

3. L'accord de sous-traitance, signé avant tout accès

3.1. Avant le premier accès. Aucun accès à des données personnelles dont vous êtes responsable n'a lieu avant la signature de l'annexe D par une personne habilitée de chaque côté. Tant qu'elle n'est pas signée, nous travaillons sur des données fictives ou anonymisées, ou nous différons l'accès (article 13.1 des CGV).

3.2. Son contenu. L'annexe D reprend ce qu'exige l'article 28.3 du RGPD, rempli pour votre mission :

- l'objet, les opérations, la finalité et la durée du traitement ;
- les catégories de personnes et de données concernées ;
- les lieux d'hébergement et d'accès, sauvegardes comprises ;
- vos instructions, les opérations permises et celles qui sont interdites ;
- les sous-traitants ultérieurs autorisés et les fournisseurs d'IA activés ;
- les mesures de sécurité retenues, avec la partie qui en a la charge ;
- le sort des données à la fin : restitution, suppression, ou les deux.

3.3. Votre modèle ou le nôtre. Nous vous remettons sur demande notre accord de sous-traitance type. Si vous préférez votre propre modèle, ou les clauses contractuelles types de la Commission européenne entre responsable et sous-traitant (décision d'exécution (UE) 2021/915), nous l'examinons et vous répondons par écrit sous 10 jours ouvrés.

3.4. Données sensibles. Santé, biométrie, opinions, données pénales et autres catégories des articles 9 et 10 du RGPD sont exclues par défaut. Elles ne sont traitées qu'après un examen préalable et des garanties écrites dans l'annexe D (article 13.3 des CGV).

4. Vos instructions et ce que nous nous interdisons

4.1. Des instructions écrites. Nous traitons vos données uniquement sur vos instructions documentées, y compris pour un transfert hors de l'Union européenne (article 28.3.a du RGPD). Une instruction nouvelle et importante (export, transfert, suppression, nouvel usage) nous parvient par écrit, de la personne désignée dans l'annexe D. Nous la confirmons par écrit avant de l'exécuter.

4.2. Une instruction contraire à la loi. Si une instruction nous paraît contraire au RGPD, nous vous en informons immédiatement (article 28.3, dernier alinéa) et suspendons l'opération concernée jusqu'à clarification. Nous n'exécutons pas une instruction illicite.

4.3. Une obligation légale. Si le droit de l'Union ou le droit français nous impose un traitement, nous vous en informons avant, sauf si ce droit l'interdit.

4.4. Nos interdits. Nous ne vendons pas vos données, ne les réutilisons ni pour notre compte ni pour un autre client, n'en constituons pas de base, ne les combinons pas avec d'autres données et ne nous en servons pas pour entraîner ou améliorer un modèle d'IA. Nous ne les envoyons à un outil d'IA tiers que sur votre instruction écrite, après retrait ou pseudonymisation de ce qui identifie une personne (IA et vos données).

---

5. Notre aide à vos obligations

Vous restez responsable de la base légale, de l'information des personnes, des durées de conservation et des réponses aux demandes. Nous vous aidons, compte tenu de la nature du traitement et des informations dont nous disposons (article 28.3.e et f du RGPD).

VOTRE OBLIGATION	CE QUE NOUS FAISONS	DÉLAI
Répondre à une personne qui exerce ses droits (articles 15 à 22)	Nous vous transmettons sa demande sans y répondre sur le fond, puis exécutons l'extraction, la rectification ou l'effacement que vous nous demandez	Transmission sous 2 jours ouvrés ; exécution sous 5 jours ouvrés
Sécuriser le traitement (article 32)	Nous appliquons les mesures convenues au point D.6 de l'annexe D et vous décrivons celles de notre périmètre	Pendant toute la mission
Notifier une violation à la CNIL et aux personnes (articles 33 et 34)	Nous vous alertons avec les informations disponibles, puis complétons à mesure que l'enquête avance	24 heures au plus après en avoir pris connaissance (point D.7)
Mener une analyse d'impact ou consulter la CNIL (articles 35 et 36)	Nous vous remettons la description du traitement, des flux, des lieux et des mesures	10 jours ouvrés après la demande
Tenir votre registre (article 30.1)	Nous vous fournissons les éléments de notre périmètre et tenons notre propre registre de sous-traitant (article 30.2)	Sur demande et à chaque changement

Sauf mandat écrit, c'est vous qui notifiez la CNIL et les personnes concernées pour les traitements dont vous êtes responsable. Les étapes et les délais d'un incident sont détaillés dans Incidents et notification. Une assistance qui dépasse la mission est chiffrée et acceptée avant, sauf si elle corrige un manquement de notre part.

---

6. Sécurité, sous-traitants ultérieurs et transferts

6.1. Personnes autorisées. Seules les personnes de BONBAY affectées à votre mission accèdent à vos données, avec un compte nominatif, la double authentification et les droits minimaux. Chacune est tenue à la confidentialité par une clause signée (article 28.3.b du RGPD). Les règles d'accès sont détaillées dans Accès à vos systèmes, nos mesures dans Sécurité de l'information.

6.2. Sous-traitants ultérieurs. Nous ne faisons appel à un autre sous-traitant qu'avec votre autorisation écrite, donnée dans l'annexe D (article 28.2). Il est tenu par contrat aux mêmes obligations que nous (article 28.4), et nous restons responsables envers vous de son exécution. Tout ajout ou remplacement vous est annoncé 30 jours avant, et vous pouvez vous y opposer. La liste, le rôle de chaque prestataire et la procédure complète sont sur la page Sous-traitants ultérieurs.

6.3. Transferts hors de l'Union européenne. Les sites et bases que nous hébergeons pour vous sont en France. Un transfert vers un pays tiers n'a lieu que sur votre instruction, s'il est indiqué dans l'annexe D et s'il repose sur un mécanisme du chapitre V du RGPD : décision d'adéquation, ou clauses contractuelles types (décision d'exécution (UE) 2021/914) avec les mesures complémentaires nécessaires. Ce qu'un fournisseur non européen change, et les options pour l'éviter, sont expliqués dans Souveraineté des données.

---

7. Audits et preuves

7.1. Les preuves d'abord. Nous tenons à votre disposition ce qui démontre le respect de nos obligations (article 28.3.h du RGPD) : accord de sous-traitance type, plan d'assurance sécurité, liste des sous-traitants ultérieurs, synthèse du dernier test d'intrusion de nos outils, attestations d'assurance responsabilité civile professionnelle et cyber. Un questionnaire RGPD ou sécurité reçoit une réponse écrite sous 10 jours ouvrés, preuves jointes.

7.2. L'audit. Vous pouvez faire contrôler une fois par an le respect de l'annexe D, sur pièces ou sur place, par vous-même ou par un auditeur indépendant tenu à la confidentialité. Nous demandons un préavis de 30 jours. Après un incident qui vous touche, ou à la demande d'une autorité de contrôle, un audit supplémentaire est possible avec le préavis minimal de 10 jours ouvrés prévu au point D.8 de l'annexe D. L'audit est à vos frais, sauf s'il révèle un manquement imputable à BONBAY.

7.3. Ses limites. L'audit ne donne accès ni aux données de nos autres clients, ni aux secrets de sécurité sans rapport avec votre traitement. La CNIL garde tous ses pouvoirs de contrôle. Le déroulé est décrit dans Conformité et audits.

---

8. Fin du contrat : restitution et suppression

8.1. Votre choix. À la fin de la mission, vous choisissez dans l'annexe D la restitution, la suppression, ou la restitution puis la suppression des données (article 28.3.g du RGPD).

8.2. Nos délais.

export de vos données dans un format ouvert sous 15 jours ouvrés après votre demande, faite avant la fin du contrat ou dans les 30 jours qui suivent (article 15 des CGV) ;
suppression de nos copies sous 30 jours après la fin du contrat, ou après la remise de l'export si vous l'avez demandé dans ce délai ;
sauvegardes effacées au terme de leur rotation de 30 jours, sans être réutilisées entre-temps ;
attestation écrite de suppression remise à la fin.

8.3. Ce que nous gardons. Seulement ce que la loi nous oblige à conserver pour nous-mêmes, comme les factures pendant 10 ans (article L123-22 du Code de commerce). Ce ne sont pas les données de vos clients ou de vos salariés. Aucune suppression définitive n'intervient avant de vous en avoir informé et de vous avoir laissé le délai de récupération convenu. La reprise de votre code et de vos accès est décrite dans Continuité et réversibilité.

---

9. Ce que cette page ne couvre pas

Vos obligations de responsable. Base légale, information des personnes, durées de conservation, registre, décision de mener une analyse d'impact, désignation d'un délégué à la protection des données : elles restent les vôtres (article 13.2 des CGV). Nous vous conseillons, sans décider à votre place. Un accompagnement complet relève d'une mission Conformité RGPD de Bonbay Cyber.
Les outils que vous administrez. Votre messagerie, votre logiciel de gestion ou un compte d'IA ouvert à votre nom : leur éditeur est votre propre sous-traitant, pas le nôtre. Vous signez avec lui son accord de l'article 28.
Les données de santé. BONBAY n'est pas certifiée hébergeur de données de santé. Si vos données relèvent de l'article L1111-8 du Code de la santé publique, elles sont hébergées chez un hébergeur certifié choisi avec vous.
La responsabilité. Un sous-traitant répond d'un dommage s'il n'a pas respecté les obligations qui lui sont propres ou s'il a agi hors de vos instructions licites (article 82.2 du RGPD). Les limites de l'article 14 des CGV s'appliquent dans la mesure permise par la loi.

Pas de délégué désigné. BONBAY n'a pas désigné de délégué à la protection des données ; Pierre Marsanne en est le référent.

10. Contact et mise à jour

10.1. Responsable. Pierre Marsanne, président de BONBAY, porte la protection des données, la sécurité et la confidentialité. Accord type, questionnaire, demande d'audit : 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 pratiques ou de la loi. Vous êtes prévenu par e-mail d'un changement qui vous concerne. Les autres pages du Centre de confiance précisent la sécurité, les accès, les incidents et la réversibilité.

10.3. Textes. Règlement (UE) 2016/679 : texte officiel sur EUR-Lex. Guides de la CNIL pour les sous-traitants : cnil.fr.