Conformité et audits.

Version 1.0 · en vigueur le 15 novembre 2026

1. Objet et portée

1.1. Ce que couvre cette page. Les référentiels que BONBAY suit, ce qu'elle ne revendique pas, ses contrôles réguliers, votre droit d'audit, le traitement de vos questionnaires, les documents remis sur demande et ses assurances.

1.2. À qui elle s'applique. Aux clients et prospects de BONBAY et de ses quatre marques (IA, Cyber, Académie, Design), à leurs acheteurs, DSI, responsables de la sécurité et délégués à la protection des données, et aux auditeurs qu'ils mandatent.

1.3. Articulation avec les autres documents. Pour le contrôle d'un traitement de données personnelles, l'article 13.6 des CGV et l'annexe D (point D.8) s'appliquent et prévalent. Le détail de nos mesures est dans Sécurité de l'information ; nos engagements de sous-traitant dans RGPD : sous-traitance ; nos engagements sociaux et environnementaux dans la charte RSE.

2. Les référentiels que nous suivons

RÉFÉRENTIEL	CE QUE NOUS EN FAISONS	STATUT
RGPD (règlement (UE) 2016/679) et loi Informatique et Libertés	Obligations de responsable de traitement et de sous-traitant (articles 28, 30 et 32 à 34)	Obligation légale
Règlement (UE) 2024/1689 sur l'IA (AI Act)	Pratiques interdites refusées (article 5), maîtrise de l'IA (article 4), transparence (article 50)	Obligation légale, selon son calendrier
ISO/IEC 27001:2022 et ISO/IEC 27002:2022	Structure de nos mesures de sécurité et de leur revue annuelle	Alignement, sans certification
Guide d'hygiène informatique de l'ANSSI	Base de nos mesures sur les postes, les comptes et les sauvegardes	Référence publique
Guide de la sécurité des données personnelles de la CNIL	Contrôle de nos mesures au regard de l'article 32 du RGPD	Référence publique

RÉFÉRENTIEL	CE QUE NOUS EN FAISONS	STATUT
Recommandations de l'ANSSI pour les systèmes d'IA générative ; classement OWASP des risques des applications de grands modèles de langage	Conception et test des outils d'IA que nous livrons	Référence publique
ISO/IEC 42001:2023	Organisation de nos pratiques d'IA : rôles, risques, revue	Référence, sans certification
ISO/IEC 29147 et ISO/IEC 30111	Notre politique de divulgation des vulnérabilités	Référence
ISO 26000 et norme VSME	Charte RSE et rapport de durabilité	Référence volontaire

2.2. Vos obligations sectorielles. Si vous êtes soumis à la directive (UE) 2022/2555 dite NIS 2 et à ses textes de transposition, au règlement (UE) 2022/2554 dit DORA, aux règles des opérateurs d'importance vitale ou de la santé, dites-le avant la commande. Les clauses que ces textes imposent à vos fournisseurs (niveaux de service, notification d'incident, droit d'audit, stratégie de sortie, sous-traitance) font l'objet d'une annexe spécifique (article 9.6 des CGV).

3. Ce que nous ne revendiquons pas

3.1. Aucune certification. BONBAY n'est pas certifiée ISO/IEC 27001 ni ISO/IEC 42001. Elle n'est pas qualifiée PASSI (prestataire d'audit de la sécurité des systèmes d'information) ni SecNumCloud, n'est pas certifiée hébergeur de données de santé (HDS) et ne détient pas le label ExpertCyber. Bonbay Académie ne mentionne la certification Qualiopi que lorsqu'elle a été délivrée, pour les catégories d'actions qu'elle couvre (mentions légales, section 4). Ce que recouvre une certification ISO 27001 est expliqué sur notre page ISO 27001.

3.2. Les certifications de nos fournisseurs. Celles d'OVHcloud, de Scaleway ou de nos fournisseurs d'IA leur appartiennent et couvrent le périmètre de leurs offres. Elles ne font pas de BONBAY une société certifiée. Nous vous indiquons l'offre utilisée, et vous pouvez vérifier son certificat auprès du fournisseur.

3.3. Quand votre projet exige une qualification. Si un texte ou votre politique d'achat impose un prestataire qualifié ou certifié (audit PASSI, hébergement HDS, offre SecNumCloud), nous le disons avant le devis et proposons un prestataire qui l'est, sous contrat avec vous ou avec nous selon l'article 2 des CGV. Sa qualification n'est jamais présentée comme la nôtre.

3.4. Si cela change. Si BONBAY obtient un jour une certification, elle publie l'organisme, le périmètre, le numéro du certificat et ses dates de validité.

4. Nos contrôles

CONTRÔLE	FRÉQUENCE	PAR QUI	CE QUE VOUS POUVEZ OBTENIR
Test d'intrusion de nos propres outils	Chaque année	Un prestataire externe indépendant, qui n'a ni conçu ni exploité les outils testés	La synthèse du dernier rapport
Revue des mesures de sécurité	Chaque année	Pierre Marsanne, président	La date et les conclusions de la dernière revue
Revue des accès	Chaque trimestre	BONBAY	La date de la dernière revue et les accès retirés
Test de restauration des sauvegardes	Chaque trimestre	BONBAY	La date et le résultat du dernier test
Test du plan de reprise	Chaque année	BONBAY	La synthèse du dernier test
Sensibilisation de toute l'équipe	Chaque année	BONBAY	La date et le programme de la dernière session
Charte et clause de confidentialité	À l'arrivée de chaque personne, partenaire et marque	Signées par chacun	Le modèle de clause

4.2. Les suites du test d'intrusion. Les failles qu'il relève sont corrigées dans les délais de notre politique de divulgation : 7 jours pour une faille critique, 30 jours pour une élevée, 90 jours pour une moyenne. La synthèse indique l'état de chaque correction.

4.3. L'indépendance. Bonbay Cyber n'audite pas les outils de BONBAY pour ce test annuel : il est confié à un prestataire externe, dont le nom figure dans la synthèse.

5. Votre droit d'audit

5.1. Fréquence et préavis. Vous pouvez auditer BONBAY une fois par an, avec un préavis de 30 jours, sur pièces (questionnaire, documents, entretiens) ou sur place, vous-même ou par un auditeur indépendant tenu à la confidentialité et sans conflit d'intérêts.

5.2. Les autres contrôles. Le contrôle ciblé de l'accord de sous-traitance prévu au point D.8 de l'annexe D reste possible aux conditions de cette annexe, avec un préavis d'au moins 10 jours ouvrés. Après un incident imputable à BONBAY, un audit supplémentaire est possible dans l'année. Les autorités de contrôle conservent tous leurs pouvoirs.

5.3. Les frais. L'audit est à vos frais, sauf s'il fait suite à un incident imputable à BONBAY ou s'il constate un manquement substantiel de sa part (article 13.6 des CGV).

5.4. Le déroulement. Le périmètre, le calendrier et les règles de sécurité sont fixés par écrit avant l'audit. Il se tient pendant les heures ouvrées et ne donne accès ni aux données d'autres clients, ni aux secrets de sécurité sans rapport avec lui. Un test intrusif sur nos outils demande en plus une autorisation écrite séparée, avec périmètre, horaires et conditions d'arrêt (article 9 des CGV).

5.5. Les suites. Vous nous remettez le rapport. Nous vous adressons un plan de correction écrit sous 30 jours après sa réception ; les failles qu'il relève suivent les délais de notre politique de divulgation.

---

6. Vos questionnaires sécurité, RGPD et RSE

6.1. Délai. Réponse écrite sous 10 jours ouvrés après réception du questionnaire, preuves jointes : extraits de nos politiques, dates et synthèses des derniers tests, attestations.

6.2. Format. Nous répondons dans votre format (tableur, document, plateforme d'évaluation des fournisseurs). Sans format imposé, vous recevez notre dossier de réponse standard, daté.

6.3. Des réponses exactes. Chaque exigence reçoit « oui », « non » ou « partiel », avec une explication. Nous ne répondons jamais « oui » à une exigence que nous n'appliquons pas. La réponse est datée et signée par Pierre Marsanne, président. Si une réponse devient inexacte pendant le contrat, nous vous le signalons.

6.4. Les questionnaires RSE et ESG. Même délai, comme l'annonce la section 10 de notre charte RSE.

6.5. Confidentialité. Certaines preuves (plan d'assurance sécurité, synthèse du test d'intrusion) sont remises sous accord de confidentialité. Une information confidentielle échangée pendant une négociation est protégée par l'article 1112-2 du Code civil, et nos informations techniques relèvent du secret des affaires (article L151-1 du Code de commerce).

---

7. Documents remis sur demande

DOCUMENT	CONTENU	CONDITIONS
Accord de sous-traitance type (annexe D des CGV)	Rôles, instructions, mesures, sous-traitants, violations, audits, fin de traitement	Libre ; signé avant tout accès à vos données personnelles
Plan d'assurance sécurité (PAS)	Mesures appliquées à votre mission, responsabilités, contacts, procédure d'incident	Sous accord de confidentialité, adapté à chaque mission

DOCUMENT	CONTENU	CONDITIONS
Liste des sous-traitants ultérieurs	Fonction, données, lieu, garanties	Publique : page Sous-traitants ultérieurs
Synthèse du dernier test d'intrusion	Périmètre, date, prestataire, nombre de failles par gravité, état des corrections	Sous accord de confidentialité ; le rapport détaillé n'est pas remis
Attestations d'assurance responsabilité civile professionnelle et cyber	Assureur, garanties, montants, période de validité	Libre
Extrait d'immatriculation et attestation de vigilance de l'URSSAF	Article L8222-1 du Code du travail	Pour un contrat de 5 000 € HT ou plus, à la conclusion puis tous les six mois (article 19.3 des CGV)
CGV, politique de données personnelles, charte RSE	Versions en vigueur et précédentes	Libre, en PDF

7.2. Délai de remise. Un document existant vous est envoyé sous 5 jours ouvrés. Un plan d'assurance sécurité propre à votre mission est rédigé avec le devis.

---

8. Nos assurances

8.1. Ce que nous avons souscrit. BONBAY est assurée en responsabilité civile professionnelle et en cyber. Chaque attestation indique l'assureur, les garanties, les montants, les franchises et la période de validité. Elle vous est remise sur demande, et de nouveau à chaque renouvellement si vous le souhaitez.

8.2. Ce qui n'y figure pas n'est pas couvert. Aucune couverture particulière, notamment cyber ou IA, n'est réputée acquise sans attestation (article 14.1 des CGV).

8.3. Assurance et responsabilité. Le plafond de responsabilité de l'article 14.1 des CGV est distinct des montants assurés. Un plafond plus élevé peut être négocié au devis, selon les enjeux et les garanties disponibles.

8.4. Nos partenaires. Thrive et Qlint, quand vous contractez directement avec eux, ont leurs propres assurances, que vous pouvez leur demander.

---

9. Limites

9.1. Une photo à une date. Un audit ou un test d'intrusion décrit un état à une date donnée, sur un périmètre défini. Il ne garantit pas l'absence de faille ou d'attaque ultérieure (article 9 des CGV).

9.2. Notre périmètre. Nos réponses couvrent les systèmes que BONBAY exploite et ses pratiques. Elles ne couvrent ni vos systèmes, ni les partenaires avec qui vous contractez directement, ni les services dont vous détenez le compte.

9.3. Pas d'avis sur votre propre conformité. Nos réponses ne valent pas analyse de la conformité de vos traitements. C'est une mission à part, par exemple un audit de cybersécurité ou un accompagnement en conformité RGPD.

9.4. Ce que nous ne remettons pas. Ni mot de passe, ni détail d'architecture qui affaiblirait la sécurité de nos outils, ni information sur d'autres clients.

9.5. L'état réel. Notre charte RSE distingue ce qui est fait, en cours ou à venir ; nos réponses à vos questionnaires suivent le même état réel.

---

10. Contact et mise à jour

10.1. Responsable. Pierre Marsanne, président de BONBAY, porte la sécurité, la confidentialité et la protection des données. Questionnaires, demandes d'audit et de documents : contact@bonbay.fr, ou BONBAY, SAS au capital de 4 500 €, 38 cours de l'Intendance, 33000 Bordeaux.

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, par exemple un nouveau contrôle ou une nouvelle assurance. Vous êtes prévenu de tout changement qui vous concerne ; une nouvelle version ne modifie pas rétroactivement un contrat en cours (article 2 des CGV).

10.3. Les autres engagements. L'ensemble des pages est réuni dans le Centre de confiance.