Politique de sécurité de l'information — Garante

Version 1.0 — 5 mai 2026

Préambule

La présente politique constitue le document fondateur du système de management de la sécurité de l'information (ci-après « **SMSI** ») mis en œuvre par Garante. Elle exprime l'engagement de la direction en matière de protection des données traitées dans le cadre du SaaS Garante et fixe le cadre des mesures techniques et organisationnelles appliquées.

Garante n'est aujourd'hui pas certifié ISO/IEC 27001:2022. La présente politique s'appuie néanmoins sur les contrôles de l'Annexe A de cette norme et sur les obligations imposées par le Règlement (UE) 2016/679 (RGPD), dans une logique de conformité progressive et d'amélioration continue.

---

1. Identification

Éditeur	Ahmed Bellafkih, exerçant sous le nom commercial Garante
Statut	Entreprise individuelle (micro-entrepreneur)
SIREN	988 920 617

Siège social	50 avenue des Champs-Élysées, 75008 Paris
Contact sécurité	security@garante.fr
Contact DPO interne	dpo@garante.fr
Périmètre du SMSI	Plateforme SaaS Garante (frontend, backend, infrastructure, sous-traitants ultérieurs)

---

2. Engagement de la direction

La direction de Garante s'engage à :

1. **Garantir la confidentialité, l'intégrité, la disponibilité et l'opposabilité** des données personnelles et professionnelles traitées par la plateforme, conformément à l'article 32 du RGPD.
2. **Allouer les ressources nécessaires** (techniques, humaines, financières) à la mise en œuvre et au maintien du SMSI, dans la mesure compatible avec la phase early-stage de l'entreprise et avec une transparence totale sur les arbitrages effectués.
3. **Respecter les engagements contractuels** pris envers les cabinets clients (Contrat de prestation SaaS, CGUV, DPA, liste des sous-traitants ultérieurs).
4. **Améliorer en continu** le niveau de sécurité par des revues régulières, l'intégration des retours d'expérience et la prise en compte des évolutions réglementaires (RGPD, recommandations CNIL et ANSSI, IA Act).
5. **Communiquer de manière honnête et publique** sur les choix de sécurité, y compris sur les éléments non encore implémentés et leur calendrier d'engagement.

---

3. Référentiel et périmètre

3.1 Référentiel suivi

- Règlement (UE) 2016/679 (**RGPD**)
- Recommandations de la **CNIL**
- Contrôles de l'**Annexe A de la norme ISO/IEC 27001:2022** (sans certification à ce jour)
- Recommandations de l'**ANSSI** applicables aux services numériques

3.2 Périmètre couvert

Le SMSI couvre :
- L'application web Garante (frontend Next.js + backend Fastify)
- L'infrastructure d'hébergement (serveur OVHcloud, France)
- Les sous-traitants ultérieurs déclarés sur la page publique `/legal/subprocessors`
- Les processus opérationnels associés (développement, déploiement, support, gestion des incidents)

3.3 Hors périmètre

- Les systèmes d'information internes des cabinets clients
- Les sous-traitants des cabinets clients (gérés directement par les cabinets dans leur propre registre)
- Les terminaux et postes de travail des utilisateurs finaux

---

4. Responsabilités

4.1 Responsable sécurité de l'information

Ahmed Bellafkih cumule, au stade actuel de l'entreprise, les fonctions de :
- Dirigeant
- Responsable sécurité de l'information (RSSI)
- DPO interne de Garante

Ce cumul transparent est documenté publiquement. Une séparation des fonctions sera engagée à l'embauche du premier collaborateur permanent.

4.2 Responsabilité des sous-traitants ultérieurs

Chaque sous-traitant ultérieur est lié contractuellement par les mêmes obligations de protection des données que celles imposées à Garante par le DPA principal (article 28(4) RGPD). La liste exhaustive et à jour est publiée sur `/legal/subprocessors`.

4.3 Responsabilité des utilisateurs

Les utilisateurs (administrateurs et collaborateurs des cabinets clients) sont tenus de respecter les bonnes pratiques de sécurité décrites dans les CGUV (mots de passe robustes, activation du 2FA, signalement immédiat de tout accès suspect).

---

5. Engagements opérationnels de sécurité

5.1 Confidentialité

- Multi-tenancy strict avec **Row-Level Security PostgreSQL** activé en production (rôle `garante_app` non superuser, NOBYPASSRLS)
- Chiffrement **AES-256-GCM** au repos pour tous les secrets sensibles en base
- Chiffrement **MinIO SSE-KMS** pour les fichiers stockés (DSAR, pièces d'identité, documents)
- **TLS 1.3** in-transit sur tous les flux externes et internes
- **2FA TOTP obligatoire par défaut** pour tous les rôles (administrateur, DPO, assistant)

5.2 Intégrité

- Audit trail tamper-evident par **chaîne de hash SHA-256** sur toutes les actions DSAR, violations, AIPD et registres (opposabilité au sens des articles 5.2 RGPD et 1366 du Code civil)
- Validation Zod systématique de chaque entrée des API
- Code source versionné Git avec historique complet et signature des commits

5.3 Disponibilité

- Sauvegardes quotidiennes chiffrées AES-256-CBC avec dérivation PBKDF2 (100 000 itérations), rétention 30 jours glissants
- Copie hors-ligne rotative quotidienne sur stockage isolé du runtime applicatif (rétention 7 jours)
- Réplication off-site géographique (souveraineté UE) : **prévue en feuille de route, non encore active**
- Procédure de restauration documentée ; **tests de restauration planifiés périodiquement** (objectif trimestriel) et lors des migrations de schéma majeures
- Service fourni en mode **best effort**, sans engagement de SLA chiffré (cf. CGUV article 13)

5.4 Opposabilité

- Audit trail SHA-256 chaîné couvrant DSAR, violations, AIPD et registres (Art. 5.2 RGPD + Art. 1366 C. civ.)
- Bundle d'export incluant manifest SHA-256 par fichier et signature globale
- Conservation des logs d'audit dans les durées définies par le DPA et la procédure de notification de violation

---

6. Engagements quantifiés

Engagement	Valeur
Délai de réponse à un signalement de faille (security.txt)	**48 heures**
Test de restauration des sauvegardes	À **chaque déploiement majeur** (incluant migration Prisma)
Audit interne de sécurité	**Annuel**
Mise à jour du registre des risques	**Annuelle** + sur événement majeur
Évaluation des sous-traitants ultérieurs (vendor assessment)	**Annuelle**
Revue de la présente politique	**Annuelle**
Délai de rédaction d'un post-mortem après incident	**30 jours**
Notification d'un incident impactant le service au client	**48 heures ouvrées**
Programme de récompense de signalement (bug bounty)	**Aucune récompense financière** — remerciement public sur demande
Formation sécurité (dirigeant et futurs collaborateurs)	**Annuelle**, auto-formation documentée
Notification d'une violation de données au client (rappel DPA Art. 4.7.1)	**48 heures** suivant détection

7. Gestion des incidents et continuité

7.1 Procédure de gestion des incidents

La procédure formalisée est documentée dans `docs/legal/procedure-notification-violation.md`. Elle s'articule en quatre étapes :
1. Détection et qualification (criticité, périmètre, données impactées)
2. Confinement et remédiation immédiate
3. Notification des parties concernées dans les délais réglementaires (48 heures pour les clients, 72 heures pour la CNIL)
4. Post-mortem écrit dans les 30 jours, intégrant les actions d'amélioration

7.2 Plan de continuité d'activité

Documenté à part. Couvre les scénarios majeurs : sinistre datacenter, attaque ransomware, indisponibilité prolongée, incapacité du dirigeant. La résiliation sans préavis est garantie en cas d'indisponibilité supérieure à 72 heures consécutives imputable à Garante (CGUV article 13.2).

8. Revue et amélioration continue

8.1 Revue de la politique

La présente politique fait l'objet d'une revue **annuelle** par la direction. Une revue exceptionnelle est déclenchée en cas d'événement majeur (incident significatif, nouveau sous-traitant ultérieur, évolution réglementaire substantielle, embauche du premier collaborateur permanent).

8.2 Indicateurs suivis

- Nombre d'incidents de sécurité par criticité
- Nombre de signalements de faille reçus et délai moyen de réponse
- Résultats des tests de restauration (succès / échec, RTO observé)
- Conformité des sous-traitants ultérieurs aux engagements contractuels (synthèse annuelle)
- Évolution des vulnérabilités identifiées dans les dépendances logicielles (rapports `npm audit`)

8.3 Documents associés

La présente politique fait partie d'un ensemble cohérent de documents :
- **Mesures techniques et organisationnelles** (`/legal/dpa` — annexe TOMs)
- **Analyse d'impact relative à la protection des données du SaaS Garante** (`/legal/aipd`)
- **Liste des sous-traitants ultérieurs** (`/legal/subprocessors`)

- **Politique de confidentialité** (`/legal/privacy`)
- **Conditions générales d'utilisation et de vente** (`/legal/terms`)
- **Contrat de prestation SaaS** (sur demande)
- **Page sécurité technique détaillée** (`/legal/securite`)

---

9. Approbation

La présente politique est approuvée et signée par :

Ahmed Bellafkih
Dirigeant et Responsable de la sécurité de l'information

Garante — SIREN 988 920 617
Fait à Paris, le 5 mai 2026

Version 1.0 — 5 mai 2026 — Prochaine revue prévue : mai 2027 (ou avant en cas d'événement majeur)