Registre des activités de traitement — Garante

Conformément aux articles 30(1) et 30(2) du Règlement (UE) 2016/679 (RGPD)

Élément	Détail
Organisme	Garante — Entreprise individuelle Ahmed Bellafkih
SIREN	988 920 617
Siège social	50 Avenue des Champs Élysées, 75008 Paris
DPO	dpo@garante.fr
Contact	contact@garante.fr
Date de rédaction	Avril 2026
Dernière mise à jour	Avril 2026
Version	1.1

Préambule

Le présent registre est tenu conformément à l'article 30 du Règlement (UE) 2016/679 (RGPD). Il documente l'ensemble des activités de traitement de données à caractère personnel effectuées par Garante, tant en qualité de **sous-traitant** (article 30(2)) pour le compte des cabinets DPO clients, qu'en qualité de **responsable de traitement** (article 30(1)) pour ses propres traitements.

Ce registre est mis à disposition de la Commission Nationale de l'Informatique et des Libertés (CNIL) sur demande, conformément à l'article 30(4) du RGPD.

PARTIE 1 — Registre du sous-traitant (Article 30(2) RGPD)

Garante agit en qualité de sous-traitant au sens de l'article 4(8) du RGPD pour le compte de cabinets de DPO externalisés (responsables de traitement). Les traitements effectués sont identiques pour chaque cabinet client et encadrés par un contrat de sous-traitance (DPA) conforme à l'article 28 du RGPD.

Fiche ST-001 — Gestion des demandes d'exercice de droits (DSAR)

Champ	Détail
Référence	ST-001
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Sous-traitant	Garante — dpo@garante.fr
Responsables de traitement	Chaque cabinet DPO client ayant souscrit un abonnement Garante (liste des cabinets tenue à jour dans la plateforme)
DPO du sous-traitant	dpo@garante.fr

Catégories de traitements effectués pour le compte du RT

1. **Réception et enregistrement** des demandes d'exercice de droits (accès, rectification, effacement, portabilité, opposition, limitation)
2. **Vérification d'identité** du demandeur (envoi de code OTP par email et/ou collecte de pièce d'identité)
3. **Data discovery** — recherche automatisée de données personnelles dans les systèmes du client via connecteurs API (HubSpot, Stripe, Brevo, Mailchimp, HTTP générique) et tâches manuelles
4. **Revue et anonymisation** assistée par intelligence artificielle (Mistral AI) — détection de données de tiers à caviarder
5. **Génération de réponses** — production de courriers PDF conformes aux articles 12 à 22 du RGPD
6. **Envoi de la réponse** au demandeur avec lien de téléchargement sécurisé et preuve de consultation (article 12(4))
7. **Archivage** — conservation du dossier complet avec piste d'audit horodatée

Catégories de données traitées

Catégorie	Données	Personnes concernées
Identité du demandeur	Nom, prénom, email, téléphone, adresse postale	Personnes exerçant leurs droits RGPD auprès des clients du cabinet
Pièce d'identité	Copie CNI ou passeport (le cas échéant)	Demandeurs DSAR
Données collectées (discovery)	Données personnelles trouvées dans les systèmes du client du cabinet	Demandeurs DSAR
Réponse DSAR	Courrier PDF, piste d'audit	Demandeurs DSAR
Communications	Messages échangés entre le demandeur et le DPO via le portail	Demandeurs DSAR

Transferts de données hors UE/EEE

AUCUN. Toutes les données sont traitées et stockées exclusivement dans l'Union européenne :
- Hébergement : Hetzner Online GmbH, Allemagne
- IA : Mistral AI SAS, France
- Emails : Brevo (Sendinblue SAS), France
- CDN / WAF / DNS : BunnyWay d.o.o. (Bunny.net), Slovénie

Sous-traitants ultérieurs

Sous-traitant	Service	Localisation	DPA
Mistral AI SAS	Analyse IA, anonymisation, génération de documents	France (UE)	Signé
Hetzner Online GmbH	Hébergement serveur dédié	Allemagne (UE)	Signé

Brevo (Sendinblue SAS)	Envoi d'emails transactionnels	France (UE)	Signé
BunnyWay d.o.o. (Bunny.net)	CDN, WAF, DNS — IPs des visiteurs portail	Slovénie (UE)	Signé

Mesures de sécurité (Article 32)

Voir le document « Mesures Techniques et Organisationnelles (TOMs) » pour le détail complet. En résumé :
- Chiffrement en transit (TLS 1.2/1.3) et au repos (AES-256-GCM)
- Multi-tenancy stricte (isolation par `cabinet_id`)
- Authentification JWT + 2FA TOTP
- Rate limiting sur les routes publiques
- Backups quotidiens chiffrés AES-256-CBC
- Logs d'audit sur chaque action DSAR
- Suppression automatique des pièces d'identité sous 30 jours

---

Fiche ST-002 — Gestion du registre des traitements (Article 30)

Champ	Détail
Référence	ST-002
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Sous-traitant	Garante — dpo@garante.fr
Responsables de traitement	Chaque cabinet DPO client

Catégories de traitements effectués pour le compte du RT

1. **Création de fiches** de traitement article 30 pour les clients du cabinet (assistée par IA)
2. **Stockage et mise à jour** des fiches de registre
3. **Calcul du score de conformité** basé sur la complétude du registre

Catégories de données traitées

Catégorie	Données	Personnes concernées
Métadonnées des fiches	Finalités, bases légales, catégories de données, destinataires, durées de conservation	N/A (métadonnées de traitements)

Transferts hors UE/EEE

AUCUN.

Mesures de sécurité

Identiques à ST-001. Voir document TOMs.

Fiche ST-003 — Audit des sous-traitants des clients

Champ	Détail
Référence	ST-003
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Sous-traitant	Garante — dpo@garante.fr
Responsables de traitement	Chaque cabinet DPO client

Catégories de traitements effectués pour le compte du RT

1. **Référencement** des sous-traitants des clients du cabinet
2. **Envoi de questionnaires** de conformité aux sous-traitants
3. **Analyse de DPA** par intelligence artificielle (vérification des 12 clauses article 28)
4. **Calcul de scores** de conformité sous-traitant

Catégories de données traitées

Catégorie	Données	Personnes concernées
Coordonnées sous-traitants	Nom société, adresse, email contact, DPO	Contacts des sous-traitants des clients
Documents contractuels	DPA, questionnaires de conformité	N/A

Transferts hors UE/EEE

AUCUN.

Fiche ST-004 — Gestion des violations de données

Champ	Détail
Référence	ST-004
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Sous-traitant	Garante — dpo@garante.fr
Responsables de traitement	Chaque cabinet DPO client

Catégories de traitements effectués pour le compte du RT

1. **Enregistrement** des déclarations de violations de données
2. **Timer 72 heures** CNIL avec alertes automatiques (H+1, H+24, H+48, H+71)
3. **Documentation** de la violation (nature, données affectées, mesures correctives)
4. **Notification** au DPO et aux personnes concernées (si risque élevé)

Catégories de données traitées

Catégorie	Données	Personnes concernées
Détails de la violation	Nature, type, date, description factuelle	N/A
Personnes affectées	Nombre et catégories de personnes concernées	Personnes concernées par la violation
Mesures correctives	Actions entreprises, statut	N/A

Transferts hors UE/EEE

AUCUN.

Fiche ST-005 — Génération de documents RGPD

Champ	Détail
Référence	ST-005
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Sous-traitant	Garante — dpo@garante.fr
Responsables de traitement	Chaque cabinet DPO client

Catégories de traitements effectués pour le compte du RT

1. **Génération** de politiques de confidentialité, procédures, notices d'information
2. **Stockage** des documents générés dans MinIO chiffré
3. **Rapports mensuels** de conformité (score, statistiques DSAR, recommandations)

Catégories de données traitées

Catégorie	Données	Personnes concernées

Contenu des documents	Textes des politiques et procédures	N/A (métadonnées)

Transferts hors UE/EEE

AUCUN.

Fiche ST-006 — Portail citoyen de dépôt de demandes

Champ	Détail
Référence	ST-006
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Sous-traitant	Garante — dpo@garante.fr
Responsables de traitement	Chaque cabinet DPO client

Catégories de traitements effectués pour le compte du RT

1. **Mise à disposition** d'un portail web public pour le dépôt de demandes d'exercice de droits
2. **Collecte** des informations du demandeur (identité, coordonnées, type de droit, justificatifs)
3. **Vérification d'identité** par code OTP email ou upload de pièce d'identité
4. **Génération** d'un accusé de réception automatique
5. **Suivi** de la demande par référence
6. **Preuve de consultation** (article 12(4) RGPD) — horodatage d'accès et adresse IP

Catégories de données traitées

Catégorie	Données	Personnes concernées
Identité	Nom, prénom, email, téléphone, adresse	Demandeurs via le portail

Pièce d'identité	Copie CNI/passeport	Demandeurs (si doute raisonnable)
Preuve de consultation	Horodatage, adresse IP	Demandeurs

Transferts hors UE/EEE

AUCUN.

PARTIE 2 — Registre du responsable de traitement (Article 30(1) RGPD)

Garante agit en qualité de responsable de traitement au sens de l'article 4(7) du RGPD pour ses propres traitements (gestion des comptes utilisateurs, facturation, logs, etc.).

Fiche RT-001 — Gestion des comptes utilisateurs

Champ	Détail
Référence	RT-001
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Responsable de traitement	Garante
DPO	dpo@garante.fr

Finalités du traitement

- Création et gestion des comptes utilisateurs de la plateforme
- Authentification et contrôle d'accès
- Gestion des rôles et permissions (admin, DPO, assistant, client_readonly)

Base légale

Exécution du contrat (article 6(1)(b) RGPD) — Le traitement est nécessaire à l'exécution du contrat d'abonnement entre Garante et le cabinet DPO.

Catégories de personnes concernées

- Utilisateurs de la plateforme Garante (DPO, assistants, administrateurs des cabinets clients)

Catégories de données

Donnée	Obligatoire	Détail
Email	Oui	Identifiant unique du compte
Nom et prénom	Oui	Identification de l'utilisateur
Mot de passe	Oui	Stocké haché (bcrypt 12 rounds) — jamais en clair
Rôle	Oui	admin, dpo, assistant, client_readonly
Secret TOTP 2FA	Non	Chiffré AES-256-GCM (si 2FA activé)
Cabinet associé	Oui	Lien multi-tenancy

Destinataires

- Équipe Garante (accès limité au besoin)
- Hetzner Online GmbH (hébergeur, stockage des données)
- BunnyWay d.o.o. (Bunny.net) — CDN/WAF/DNS, traite les IPs et headers HTTP des connexions

Transferts hors UE/EEE

AUCUN.

Durées de conservation

Donnée	Durée	Justification
Compte actif	Durée de l'abonnement	Exécution du contrat
Compte supprimé	2 ans après suppression	Prescription contractuelle

Mesures de sécurité

- Mots de passe hachés bcrypt 12 rounds avec politique de complexité (min. 8 caractères, majuscule, minuscule, chiffre, caractère spécial)
- JWT access token 15 min, refresh token 7 jours
- Cookies HttpOnly, Secure, SameSite=Strict
- 2FA TOTP optionnel (recommandé pour les administrateurs)
- Multi-tenancy stricte par `cabinet_id`

Fiche RT-002 — Logs techniques et sécurité

Champ	Détail
Référence	RT-002
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Responsable de traitement	Garante
DPO	dpo@garante.fr

Finalités du traitement

- Détection et prévention des incidents de sécurité
- Traçabilité des actions (audit trail)
- Débogage et amélioration du service
- Détection des accès non autorisés

Base légale

Intérêt légitime (article 6(1)(f) RGPD) — Sécurité des systèmes d'information et protection des données des utilisateurs et des personnes concernées.

Catégories de personnes concernées

- Utilisateurs de la plateforme Garante
- Visiteurs du portail public DSAR

Catégories de données

Donnée	Détail
Adresse IP	Source de la requête
User-agent	Navigateur et système d'exploitation
Timestamps	Horodatage de chaque requête
Action effectuée	Type d'opération (création, lecture, modification, suppression)
Résultat	Succès ou échec de l'opération

Note : Les paramètres sensibles (mots de passe, tokens, secrets) sont systématiquement masqués dans les logs.

Destinataires

- Équipe technique Garante (accès restreint)
- Hetzner Online GmbH (hébergeur)
- BunnyWay d.o.o. (Bunny.net) — logs d'accès CDN/WAF (IP, headers, user-agent)

Transferts hors UE/EEE

AUCUN.

Durées de conservation

Type de log	Durée	Justification
Logs HTTP applicatifs	12 mois	Référentiel CNIL
Logs d'audit DSAR	5 ans	Preuve de conformité RGPD
Logs d'audit vault	12 mois	Traçabilité accès secrets
Logs d'audit IA	12 mois	Traçabilité des appels Mistral AI
Logs d'accès Bunny (CDN/WAF)	Selon politique Bunny.net (UE)	Sécurité/anti-DDoS

Mesures de sécurité

- Format JSON structuré (Pino)
- Masquage automatique des paramètres sensibles
- Accès restreint à l'équipe technique
- Stockage sur serveur dédié Hetzner (Allemagne)

Fiche RT-003 — Emails transactionnels

Champ	Détail
Référence	RT-003
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Responsable de traitement	Garante
DPO	dpo@garante.fr

Finalités du traitement

- Envoi d'emails transactionnels liés au fonctionnement du service (accusés de réception, codes OTP, notifications, alertes SLA, réponses DSAR)
- Suivi de la délivrabilité (tracking ouverture et clics)

Base légale

Exécution du contrat (article 6(1)(b) RGPD) — Les emails transactionnels sont nécessaires au fonctionnement du service.

Catégories de personnes concernées

- Utilisateurs de la plateforme Garante
- Demandeurs DSAR (via le portail)
- Sous-traitants des clients du cabinet (relances questionnaires)

Catégories de données

Donnée	Détail
Adresse email destinataire	Pour l'envoi
Sujet de l'email	Objet du message
Contenu	Corps du message
Statut de livraison	Envoyé, délivré, ouvert, cliqué, erreur
Tracking	Pixel ouverture + clics

Destinataires

- Brevo (Sendinblue SAS) — envoi des emails en mode garante par défaut
- SMTP personnalisé du cabinet (le cas échéant)

Transferts hors UE/EEE

AUCUN. Brevo traite les données en France.

Durées de conservation

Donnée	Durée	Justification
Logs d'envoi	12 mois	Traçabilité et débogage
Statistiques agrégées	Durée de l'abonnement	Reporting

Fiche RT-004 — Facturation et comptabilité

Champ	Détail
Référence	RT-004
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Responsable de traitement	Garante
DPO	dpo@garante.fr

Finalités du traitement

- Facturation des abonnements
- Suivi des paiements
- Respect des obligations comptables et fiscales

Base légale

Obligation légale (article 6(1)(c) RGPD) — Obligations comptables et fiscales (Code général des impôts, Code de commerce article L123-22).

Catégories de personnes concernées

- Cabinets DPO clients (personnes morales et leurs représentants)

Catégories de données

Donnée	Détail
Raison sociale du cabinet	Identification
SIREN/SIRET	Identification fiscale
Adresse de facturation	Établissement de la facture
Coordonnées du contact facturation	Email, téléphone
Historique des paiements	Montants, dates, statuts
Factures	Documents comptables

Destinataires

- Service comptable Garante
- Expert-comptable (le cas échéant)
- Stripe Inc. (prestataire de paiement)

Transferts hors UE/EEE

Stripe Inc. (États-Unis) — encadré par le Data Privacy Framework (DPF) et par les clauses contractuelles types (CCT) adoptées par la Commission européenne.

Durées de conservation

Donnée	Durée	Justification
Factures et pièces comptables	10 ans	Article L123-22 Code de commerce
Données de paiement	13 mois après la date de débit	Recommandation CNIL

Fiche RT-005 — Audit des accès aux secrets (vault)

Champ	Détail

Référence	RT-005
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Responsable de traitement	Garante
DPO	dpo@garante.fr

Finalités du traitement

- Traçabilité des accès au coffre-fort de secrets (Infisical)
- Détection d'accès non autorisés aux secrets applicatifs
- Conformité aux bonnes pratiques de sécurité

Base légale

Intérêt légitime (article 6(1)(f) RGPD) — Sécurité des systèmes d'information.

Catégories de personnes concernées

- Système applicatif Garante (accès automatisés)
- Administrateurs techniques (le cas échéant)

Catégories de données

Donnée	Détail
Clé accédée	Nom de la variable de configuration (jamais la valeur)
Timestamp	Date et heure de l'accès
Source	Service demandeur

Transferts hors UE/EEE

AUCUN. Infisical est auto-hébergé sur le même serveur Hetzner.

Durées de conservation

12 mois.

Fiche RT-006 — Audit des appels à l'intelligence artificielle

Champ	Détail
Référence	RT-006
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Responsable de traitement	Garante
DPO	dpo@garante.fr

Finalités du traitement

- Traçabilité des appels à Mistral AI
- Mesure de la performance et des coûts (tokens consommés)
- Détection d'anomalies

Base légale

Intérêt légitime (article 6(1)(f) RGPD) — Traçabilité, sécurité et optimisation du service.

Catégories de personnes concernées

- Utilisateurs de la plateforme (indirectement, via les fonctions IA qu'ils déclenchent)

Catégories de données

Donnée	Détail
Fonction appelée	Type d'opération IA (agrégation, anonymisation, rédaction, registre, DPA)

Résumé du prompt	Description abrégée (pas le prompt complet)
Latence	Temps de réponse en millisecondes
Tokens consommés	Nombre de tokens entrée/sortie
Timestamp	Date et heure de l'appel
Utilisateur déclencheur	ID de l'utilisateur ayant déclenché la fonction

Note : Mistral AI opère avec une politique de confidentialité protégeant les données — les données envoyées ne sont pas utilisées pour l'entraînement du modèle.

Transferts hors UE/EEE

Aucun transfert hors UE. Mistral AI SAS traite les données en France.

Durées de conservation

12 mois.

Fiche RT-007 — Cookies et mesure d'audience du site web

Champ	Détail
Référence	RT-007
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Responsable de traitement	Garante
DPO	dpo@garante.fr

Finalités du traitement

- Mesure d'audience du site garante.fr (pages vues, durée, parcours)
- Amélioration de l'ergonomie et du contenu du site

Base légale

Consentement (article 6(1)(a) RGPD) pour les cookies analytics non exemptés.
Intérêt légitime (article 6(1)(f) RGPD) pour les cookies strictement nécessaires au fonctionnement du site.

Catégories de personnes concernées

- Visiteurs du site garante.fr

Catégories de données

Donnée	Détail
Identifiants techniques	Cookie ID, session ID
Navigation	Pages visitées, durée, parcours, source d'arrivée
Données techniques	Type de navigateur, résolution, système d'exploitation

Note : Garante n'utilise actuellement aucune solution de mesure d'audience tiers. BunnyWay d.o.o. (Bunny.net) intervient en tant que CDN/WAF et traite les IPs et headers HTTP à des fins de sécurité (DDoS, OWASP) ; ces données ne sont pas utilisées pour de la mesure d'audience.

Transferts hors UE/EEE

AUCUN (Bunny.net traite les données dans l'UE — Slovénie + nœuds CDN UE).

Durées de conservation

Donnée	Durée	Justification
Cookies analytics	13 mois maximum	Lignes directrices CNIL 17 septembre 2020
Données agrégées	25 mois	Analyse de tendance

Fiche RT-008 — Prospection commerciale B2B

Champ	Détail
Référence	RT-008
Date de création	Avril 2026
Dernière mise à jour	Avril 2026
Responsable de traitement	Garante
DPO	dpo@garante.fr

Finalités du traitement

- Prospection commerciale B2B auprès de cabinets DPO et professionnels de la conformité
- Gestion de la relation prospect (suivi, relances, démonstrations)
- Communication commerciale (newsletter, annonces produit)

Base légale

Intérêt légitime (article 6(1)(f) RGPD) — Prospection B2B auprès de professionnels dans le cadre de leur activité professionnelle. Conformément aux recommandations CNIL, la sollicitation B2B par email est autorisée sans consentement préalable si elle concerne l'activité professionnelle du destinataire et respecte le droit d'opposition.

Catégories de personnes concernées

- Professionnels DPO et conformité contactés dans le cadre de leur activité (LinkedIn, événements, formulaires site)

Catégories de données

Donnée	Détail
Identité professionnelle	Nom, prénom, titre/fonction
Coordonnées professionnelles	Email professionnel, téléphone professionnel, profil LinkedIn

Entreprise	Nom du cabinet, taille, secteur
Interactions	Historique des échanges, démonstrations, intérêt exprimé
Source	Canal d'acquisition (LinkedIn, événement, site web, recommandation)

Destinataires

- Équipe commerciale Garante

Transferts hors UE/EEE

AUCUN.

Durées de conservation

Donnée	Durée	Justification
Prospects actifs	3 ans à compter du dernier contact	Référentiel CNIL prospection B2B
Prospects inactifs	Suppression après 3 ans sans interaction	Référentiel CNIL
Données de désabonnement (liste d'opposition)	Durée illimitée	Respect du droit d'opposition

Mesures de sécurité

- Accès restreint à l'équipe commerciale
- Lien de désabonnement dans chaque communication commerciale
- Droit d'opposition respecté sous 48h

ANNEXE — Résumé des mesures de sécurité (Article 32 RGPD)

Pour le détail complet des mesures techniques et organisationnelles, se référer au document « TOMs — Mesures Techniques et Organisationnelles ».

Domaine	Mesures
Chiffrement en transit	TLS 1.2/1.3 (Nginx), HSTS activé
Chiffrement au repos	MinIO SSE AES-256-GCM, backups AES-256-CBC, secrets AES-256-GCM
Authentification	JWT (access 15min / refresh 7j), cookies HttpOnly Secure SameSite=Strict
2FA	TOTP optionnel (otplib v13), recommandé pour les administrateurs
Contrôle d'accès	Multi-tenancy stricte (cabinet_id), 4 rôles (admin, dpo, assistant, client_readonly)
Rate limiting	5 req/15min/IP (login), 5 req/IP/h (portail public)
Validation	Zod sur chaque input API, Prisma (requêtes paramétrées)
Backups	pg_dump quotidien + volumes MinIO, chiffrés AES-256-CBC, rétention 30 jours
Audit	4 tables d'audit (DSAR, vault, IA, HTTP)
Pièces d'identité	Suppression automatique sous 30 jours (cron quotidien)
Secrets	Infisical vault, rafraîchissement cron toutes les 5 minutes

---

Document généré en avril 2026 — Garante
Ce registre doit être mis à jour à chaque évolution des traitements.