Garante

Plateforme de gestion RGPD pour cabinets DPO

CONTRAT DE SOUS-TRAITANCE DE DONNEES A CARACTERE PERSONNEL

Au sens de l'article 28 du Reglement (UE) 2016/679 du Parlement europeen et du Conseil du 27 avril 2016 relatif a la protection des personnes physiques a l'egard du traitement des donnees a caractere personnel et a la libre circulation de ces donnees (ci-apres le "RGPD")

ENTRE LES SOUSSIGNES

Garante, entreprise individuelle exploitee par Ahmed Bellafkih, immatriculee sous le numero SIREN 988 920 617, dont le siege est situe au 50 Avenue des Champs Elysees, 75008 Paris, representee par Ahmed Bellafkih, en sa qualite d'exploitant individuel,

Ci-apres denommee **"le Sous-traitant"** ou **"Garante"**,

D'UNE PART,

ET

[A COMPLETER -- Raison sociale du cabinet DPO], societe [A COMPLETER] au capital de [A COMPLETER] euros, immatriculee au RCS de [A COMPLETER] sous le numero [A COMPLETER -- SIREN], dont le siege social est sis [A COMPLETER], representee par [A COMPLETER], en sa qualite de [A COMPLETER],

Ci-apres denommee **"le Responsable de traitement"** ou **"le Cabinet"**,

D'AUTRE PART,

Ci-apres individuellement designees une **"Partie"** et collectivement les **"Parties"**.

PREAMBULE

Le Responsable de traitement exerce l'activite de Delegue a la Protection des Donnees externalise au sens de l'article 37 du RGPD pour le compte de ses propres clients (ci-apres les "Clients du Cabinet").

Dans le cadre de cette activite, le Responsable de traitement a souscrit un abonnement a la plateforme Garante, solution SaaS (Software as a Service) editee par le Sous-traitant, destinee a automatiser et

centraliser la gestion de la conformite RGPD, et notamment le traitement des demandes d'exercice de droits (DSAR), la tenue du registre des traitements, l'audit des sous-traitants, la gestion des violations de donnees et la generation de documents de conformite.

Le present contrat a pour objet de definir les conditions dans lesquelles le Sous-traitant s'engage a effectuer, pour le compte du Responsable de traitement, les operations de traitement de donnees a caractere personnel necessaires a la fourniture du Service, conformement aux dispositions de l'article 28 du RGPD et de la loi n. 78-17 du 6 janvier 1978 modifiee relative a l'informatique, aux fichiers et aux libertes (ci-apres la "Loi Informatique et Libertes").

Le present contrat est etabli par ecrit, y compris sous forme electronique, conformement a l'article 28, paragraphe 9, du RGPD.

ARTICLE 1 -- DEFINITIONS

"Donnees a caractere personnel" ou **"Donnees personnelles"** : toute information se rapportant a une personne physique identifiee ou identifiable, au sens de l'article 4(1) du RGPD.

"Traitement" : toute operation ou tout ensemble d'operations effectuees ou non a l'aide de procedes automatises et appliquees a des donnees a caractere personnel, au sens de l'article 4(2) du RGPD.

"Personne concernee" : la personne physique dont les donnees a caractere personnel font l'objet d'un traitement.

"Violation de donnees a caractere personnel" : une violation de la securite entrainant, de maniere accidentelle ou illicite, la destruction, la perte, l'alteration, la divulgation non autorisee de donnees a caractere personnel transmises, conservees ou traitees d'une autre maniere, ou l'acces non autorise a de telles donnees, au sens de l'article 4(12) du RGPD.

"Sous-traitant ulterieur" : tout sous-traitant recrute par le Sous-traitant pour mener des activites de traitement specifiques pour le compte du Responsable de traitement.

"Service" ou **"Plateforme"** : la plateforme SaaS Garante et l'ensemble des fonctionnalites mises a disposition du Responsable de traitement dans le cadre de son abonnement.

"DSAR" (Data Subject Access Request) : demande d'exercice de droits au sens des articles 15 a 22 du RGPD.

ARTICLE 2 -- OBJET

2.1. Le present contrat definit les obligations respectives des Parties en matiere de protection des donnees a caractere personnel traitees par le Sous-traitant pour le compte du Responsable de traitement dans le cadre de la fourniture du Service.

2.2. Le Sous-traitant s'engage a traiter les Donnees personnelles uniquement pour la (les) finalite(s) qui fait (font) l'objet de la sous-traitance, telles que decrites a l'Annexe 1, et conformement aux instructions

documentees du Responsable de traitement figurant a l'Annexe 4.

2.3. Le present contrat fait partie integrante du contrat principal d'abonnement au Service Garante (ci-apres le "Contrat Principal"). En cas de contradiction entre le present contrat et le Contrat Principal, les dispositions du present contrat prevalent en ce qui concerne la protection des donnees a caractere personnel.

ARTICLE 3 -- DUREE

3.1. Le present contrat prend effet a la date de sa signature et demeure en vigueur pendant toute la duree du Contrat Principal d'abonnement au Service.

3.2. Le present contrat est automatiquement renouvele dans les memes conditions que le Contrat Principal, sauf denonciation par l'une des Parties dans les conditions prevues au Contrat Principal.

3.3. Les obligations de confidentialite, les dispositions relatives au sort des donnees en fin de contrat (Article 10) et les obligations d'assistance en cas de controle de la CNIL survivent a l'expiration ou a la resiliation du present contrat.

ARTICLE 4 -- OBLIGATIONS DU SOUS-TRAITANT

4.1. Traitement sur instruction documentee

4.1.1. Le Sous-traitant ne traite les Donnees personnelles que sur instruction documentee du Responsable de traitement, y compris en ce qui concerne les transferts de donnees vers un pays tiers ou une organisation internationale, a moins qu'il ne soit tenu d'y proceder en vertu du droit de l'Union europeenne ou du droit de l'Etat membre auquel il est soumis. Dans ce cas, le Sous-traitant informe le Responsable de traitement de cette obligation juridique avant le traitement, sauf si le droit concerne interdit une telle information pour des motifs importants d'interet public.

4.1.2. Le Sous-traitant informe immediatement le Responsable de traitement si, selon lui, une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l'Union europeenne ou du droit francais relative a la protection des donnees.

4.1.3. Les instructions du Responsable de traitement figurent a l'Annexe 4 du present contrat. Toute instruction supplementaire ou modification doit etre transmise par ecrit (y compris par courrier electronique).

4.2. Obligation de confidentialite

4.2.1. Le Sous-traitant veille a ce que les personnes autorisees a traiter les Donnees personnelles :

- s'engagent a respecter la confidentialite ou soient soumises a une obligation legale appropriee de confidentialite ;

- recoivent la formation necessaire en matiere de protection des donnees a caractere personnel.

4.2.2. Le Sous-traitant prend les mesures necessaires pour que seules les personnes ayant besoin d'acceder aux Donnees personnelles dans le cadre de l'execution du Service y aient effectivement acces (principe du moindre privilege).

4.3. Securite du traitement

4.3.1. Le Sous-traitant met en oeuvre les mesures techniques et organisationnelles appropriees afin de garantir un niveau de securite adapte au risque, conformement a l'article 32 du RGPD. Ces mesures comprennent notamment, selon les besoins :

a) la pseudonymisation et le chiffrement des Donnees personnelles ;

b) des moyens permettant de garantir la confidentialite, l'integrite, la disponibilite et la resilience constantes des systemes et des services de traitement ;

c) des moyens permettant de retablir la disponibilite des Donnees personnelles et l'acces a celles-ci dans des delais appropries en cas d'incident physique ou technique ;

d) une procedure visant a tester, a analyser et a evaluer regulierement l'efficacite des mesures techniques et organisationnelles pour assurer la securite du traitement.

4.3.2. En particulier, le Sous-traitant garantit que les donnees transmises au service d'intelligence artificielle (Mistral AI) sont traitees en mode **Zero Data Retention (ZDR)** : les donnees ne sont ni conservees apres traitement, ni utilisees pour l'entrainement du modele. Seules les donnees strictement necessaires au traitement sont transmises.

4.3.3. Le detail des mesures techniques et organisationnelles mises en oeuvre par le Sous-traitant est decrit a l'Annexe 3 du present contrat.

4.3.4. Le Sous-traitant s'engage a reexaminer et, le cas echeant, a mettre a jour ces mesures periodiquement, en tenant compte de l'etat des connaissances, des couts de mise en oeuvre, de la nature, de la portee, du contexte et des finalites du traitement, ainsi que des risques pour les droits et libertes des personnes physiques.

4.4. Sous-traitance ulterieure

4.4.1. Le Responsable de traitement autorise de maniere generale le Sous-traitant a recruter des sous-traitants ulterieurs pour l'execution de services specifiques, sous reserve du respect des conditions prevues au present article. La liste des sous-traitants ulterieurs autorises a la date de signature du present contrat figure a l'Annexe 2.

4.4.2. Le Sous-traitant informe le Responsable de traitement de tout projet de changement concernant l'ajout ou le remplacement d'un sous-traitant ulterieur. Cette information est communiquee par ecrit (y compris par courrier electronique) au moins **trente (30) jours calendaires** avant la date envisagee de mise en oeuvre du changement, afin de permettre au Responsable de traitement de formuler ses objections.

4.4.3. En cas d'objection du Responsable de traitement, les Parties se concertent de bonne foi pour trouver une solution alternative. A defaut d'accord dans un delai de quinze (15) jours ouvrables a compter de la reception de l'objection, le Responsable de traitement peut resilier le present contrat et le Contrat Principal moyennant un preavis de trente (30) jours, sans penalite.

4.4.4. Le Sous-traitant impose contractuellement a tout sous-traitant ulterieur, par voie d'un contrat ecrit, les memes obligations en matiere de protection des donnees que celles prevues au present contrat, en particulier la presentation de garanties suffisantes quant a la mise en oeuvre de mesures techniques et organisationnelles appropriees.

4.4.5. Lorsqu'un sous-traitant ulterieur ne remplit pas ses obligations en matiere de protection des donnees, le Sous-traitant demeure pleinement responsable devant le Responsable de traitement de l'execution des obligations dudit sous-traitant ulterieur.

4.5. Assistance pour l'exercice des droits des personnes concernees

4.5.1. Le Sous-traitant aide le Responsable de traitement, par des mesures techniques et organisationnelles appropriees, dans toute la mesure du possible, a s'acquitter de son obligation de donner suite aux demandes dont les personnes concernees le saisissent en vue d'exercer leurs droits prevus au chapitre III du RGPD (articles 15 a 22), et notamment les droits d'acces, de rectification, d'effacement, de limitation du traitement, de portabilite et d'opposition.

4.5.2. Lorsque le Sous-traitant recoit directement une demande d'exercice de droits de la part d'une personne concernee, il en informe le Responsable de traitement dans un delai maximum de **quarante-huit (48) heures** et ne donne pas suite a la demande sans instruction prealable du Responsable de traitement, sauf obligation legale contraire.

4.5.3. La Plateforme Garante met a disposition du Responsable de traitement les outils techniques necessaires pour faciliter le traitement des demandes d'exercice de droits, et notamment : portail de depot, verification d'identite, recherche automatisee de donnees (data discovery), anonymisation assistee par IA, generation de reponses et archivage avec piste d'audit.

4.6. Assistance pour les obligations de securite et de conformite

4.6.1. Le Sous-traitant aide le Responsable de traitement a garantir le respect des obligations prevues aux articles 32 a 36 du RGPD, compte tenu de la nature du traitement et des informations a la disposition du Sous-traitant, et notamment :

a) la securite du traitement (article 32) ;

b) la notification des violations de donnees a caractere personnel a l'autorite de controle (article 33) ;

c) la communication d'une violation de donnees a caractere personnel a la personne concernee (article 34) ;

d) la realisation d'analyses d'impact relatives a la protection des donnees (article 35) ;

e) la consultation prealable de l'autorite de controle (article 36).

4.7. Notification des violations de donnees a caractere personnel

4.7.1. Le Sous-traitant notifie au Responsable de traitement toute violation de donnees a caractere personnel dans un delai maximum de **quarante-huit (48) heures** apres en avoir pris connaissance, par tout moyen permettant d'en attester la reception (courrier electronique avec accuse de reception, notification via la Plateforme).

4.7.2. Cette notification comprend au minimum les informations suivantes, ou a defaut celles qui sont disponibles au moment de la notification, les informations complementaires etant communiquees dans les meilleurs delais :

a) la description de la nature de la violation de donnees, y compris, si possible, les categories et le nombre approximatif de personnes concernees ainsi que les categories et le nombre approximatif d'enregistrements de donnees concernes ;

b) le nom et les coordonnees du point de contact aupres duquel des informations supplementaires peuvent etre obtenues ;

c) la description des consequences probables de la violation ;

d) la description des mesures prises ou que le Sous-traitant propose de prendre pour remedier a la violation, y compris, le cas echeant, les mesures pour en attenuer les eventuelles consequences negatives.

4.7.3. Le Sous-traitant consigne toute violation de donnees a caractere personnel, en indiquant les faits concernant la violation, ses effets et les mesures prises pour y remedier. Cette documentation est mise a la disposition du Responsable de traitement sur demande.

4.7.4. La procedure detaillee de notification des violations figure a l'Annexe 5 du present contrat.

4.8. Registre des categories d'activites de traitement

Le Sous-traitant tient un registre de toutes les categories d'activites de traitement effectuees pour le compte du Responsable de traitement, conformement a l'article 30, paragraphe 2, du RGPD, comprenant :

a) le nom et les coordonnees du Sous-traitant et de chaque Responsable de traitement pour le compte duquel il agit, ainsi que, le cas echeant, les noms et les coordonnees du delegue a la protection des donnees ;

b) les categories de traitements effectues pour le compte de chaque Responsable de traitement ;

c) le cas echeant, les transferts de Donnees personnelles vers un pays tiers ou a une organisation internationale ;

d) dans la mesure du possible, une description generale des mesures de securite techniques et organisationnelles visees a l'article 32, paragraphe 1.

4.9. Designation d'un delegue a la protection des donnees

Le Sous-traitant communique au Responsable de traitement les coordonnees de son delegue a la protection des donnees ou, a defaut, de la personne en charge des questions relatives a la protection des donnees a caractere personnel :

- **Email** : dpo@garante.fr

4.10. Protection des donnees des la conception et par defaut

Le Sous-traitant met en oeuvre les principes de protection des donnees des la conception et de protection des donnees par defaut, conformement a l'article 25 du RGPD. A ce titre, la Plateforme Garante integre notamment :

a) une architecture multi-tenancy avec isolation stricte des donnees par cabinet (cabinet_id) ;

b) un chiffrement des donnees sensibles au niveau applicatif (AES-256-GCM) ;

c) une suppression automatique des pieces d'identite apres trente (30) jours ;

d) une collecte limitee aux donnees strictement necessaires a la fourniture du Service.

ARTICLE 5 -- OBLIGATIONS DU RESPONSABLE DE TRAITEMENT

5.1. Le Responsable de traitement fournit au Sous-traitant les instructions documentees relatives au traitement des Donnees personnelles, conformement a l'Annexe 4.

5.2. Le Responsable de traitement veille, prealablement et pendant toute la duree du traitement, au respect des obligations prevues par le RGPD et la Loi Informatique et Libertes, et notamment a la licite du traitement des Donnees personnelles transmises au Sous-traitant.

5.3. Le Responsable de traitement supervise le traitement, y compris en realisant les audits et inspections prevus a l'Article 6 du present contrat.

5.4. Le Responsable de traitement informe le Sous-traitant de toute modification substantielle des instructions ou de tout changement impactant le traitement des Donnees personnelles.

ARTICLE 6 -- DROIT D'AUDIT

6.1. Le Sous-traitant met a la disposition du Responsable de traitement toutes les informations necessaires pour demontrer le respect de l'ensemble des obligations prevues au present contrat et decoulant de l'article 28 du RGPD, et pour permettre la realisation d'audits, y compris des inspections, par le Responsable de traitement ou un autre auditeur qu'il a mandate, et contribue a ces audits.

6.2. Les audits sont realises dans les conditions suivantes :

a) le Responsable de traitement adresse une demande ecrite au Sous-traitant au moins **quinze (15) jours ouvrables** avant la date envisagee de l'audit ;

b) les audits sont realises pendant les heures ouvrables et de maniere a ne pas perturber de maniere disproportionnee les activites du Sous-traitant ;

c) le Responsable de traitement peut realiser ou faire realiser **un (1) audit par annee civile**, sauf en cas de violation de donnees ou de demande de l'autorite de controle ;

d) les resultats de l'audit sont communiques au Sous-traitant dans un delai raisonnable ;

e) les frais de l'audit sont a la charge du Responsable de traitement, sauf si l'audit revele un manquement substantiel du Sous-traitant aux obligations du present contrat, auquel cas les frais sont a la charge du Sous-traitant.

6.3. Le Sous-traitant informe immediatement le Responsable de traitement si, a son avis, une instruction relative a un audit est susceptible de constituer une violation du RGPD ou de toute autre disposition du droit applicable.

ARTICLE 7 -- LOCALISATION ET TRANSFERTS DE DONNEES

7.1. Les Donnees personnelles traitees dans le cadre du present contrat sont exclusivement hebergees et traitees au sein de l'Union europeenne / Espace economique europeen, et plus precisement :

Lieu de traitement	Prestataire	Pays	Objet
Data center	Hetzner Online GmbH	Allemagne	Hebergement de la Plateforme et des donnees
IA / LLM	Mistral AI SAS	France	Analyse, anonymisation, generation de documents
Emails transactionnels	Brevo (Sendinblue SAS)	France	Envoi d'emails pour le compte du Service
CDN / WAF / DNS	BunnyWay d.o.o. (Bunny.net)	Slovenie	Acceleration performance, protection DDoS/WAF, resolution DNS

7.2. Le Sous-traitant s'interdit de transferer les Donnees personnelles en dehors de l'Union europeenne / Espace economique europeen sans l'accord prealable et ecrit du Responsable de traitement.

7.3. En cas de necessite de transfert vers un pays tiers, le Sous-traitant s'engage a mettre en place les garanties appropriees conformement au chapitre V du RGPD, et notamment les clauses contractuelles types adoptees par la Commission europeenne ou toute autre garantie reconnue.

ARTICLE 8 -- RESPONSABILITE

8.1. Chaque Partie repond de ses propres manquements aux obligations qui lui incombent en vertu du present contrat et de la reglementation applicable en matiere de protection des donnees a caractere personnel.

8.2. La responsabilite totale du Sous-traitant au titre du present contrat est limitee, toutes causes confondues, au montant total des sommes effectivement versees par le Responsable de traitement au titre du Contrat Principal au cours des **douze (12) mois** precedant l'evenement a l'origine du dommage.

8.3. En aucun cas, le Sous-traitant ne pourra etre tenu responsable des dommages indirects, tels que pertes de chiffre d'affaires, perte de clientele, perte de donnees (hors manquement a ses obligations de securite), prejudice d'image ou perte de chance.

8.4. Les limitations de responsabilite prevues au present article ne s'appliquent pas en cas de faute lourde ou intentionnelle du Sous-traitant, ni en cas de violation des obligations de confidentialite ou des dispositions relatives aux transferts de donnees.

ARTICLE 9 -- CONFIDENTIALITE

9.1. Chaque Partie s'engage a garder strictement confidentielles les informations et documents de quelque nature que ce soit, relatifs a l'autre Partie, dont elle aurait eu connaissance a l'occasion de la conclusion et de l'execution du present contrat.

9.2. Cette obligation de confidentialite subsiste pendant toute la duree du contrat et pendant une duree de **cinq (5) ans** suivant son expiration ou sa resiliation.

ARTICLE 10 -- SORT DES DONNEES EN FIN DE CONTRAT

10.1. A l'expiration ou a la resiliation du present contrat, quelle qu'en soit la cause, le Sous-traitant s'engage, au choix du Responsable de traitement exprime par ecrit dans un delai de **trente (30) jours** suivant la fin du contrat :

a) a **restituer** l'integralite des Donnees personnelles au Responsable de traitement dans un format structure, couramment utilise et lisible par machine (JSON ou CSV) ; ou

b) a **supprimer** l'integralite des Donnees personnelles et a detruire toutes les copies existantes.

10.2. Le Sous-traitant delivre au Responsable de traitement une **attestation ecrite de destruction** des Donnees personnelles dans un delai de **quinze (15) jours ouvrables** suivant la destruction effective.

10.3. A defaut de choix exprime par le Responsable de traitement dans le delai prevu au paragraphe 10.1, le Sous-traitant procede a la suppression des Donnees personnelles a l'issue d'un delai de **soixante (60) jours** suivant la fin du contrat.

10.4. Par exception, le Sous-traitant peut conserver certaines Donnees personnelles lorsque le droit de l'Union europeenne ou le droit francais en impose la conservation. Dans ce cas, le Sous-traitant informe le Responsable de traitement de cette obligation et des donnees concernees.

ARTICLE 11 -- COOPERATION EN CAS DE CONTROLE DE LA CNIL

11.1. En cas de controle, d'enquete ou de demande d'information de la Commission Nationale de l'Informatique et des Libertes (CNIL) ou de toute autre autorite de controle competente portant sur les traitements objet du present contrat, le Sous-traitant s'engage a :

a) informer le Responsable de traitement dans un delai maximum de **quarante-huit (48) heures** apres avoir ete informe du controle, sauf si l'autorite de controle s'y oppose ;

b) cooperer pleinement avec l'autorite de controle et le Responsable de traitement ;

c) mettre a disposition de l'autorite de controle toutes les informations et documents necessaires concernant les traitements effectues pour le compte du Responsable de traitement ;

d) faciliter l'acces de l'autorite de controle aux locaux, equipements et systemes pertinents ;

e) ne prendre aucune mesure susceptible de compromettre le controle.

11.2. Les obligations de cooperation du present article survivent a l'expiration ou a la resiliation du present contrat.

ARTICLE 12 -- DROIT APPLICABLE ET JURIDICTION

12.1. Le present contrat est regi par le droit francais.

12.2. Tout differend relatif a la validite, l'interpretation ou l'execution du present contrat sera soumis a la competence exclusive des tribunaux de Paris, nonobstant pluralite de defendeurs ou appel en garantie.

ARTICLE 13 -- DISPOSITIONS DIVERSES

13.1. **Integralite** -- Le present contrat, y compris ses annexes, constitue l'integralite de l'accord entre les Parties concernant la protection des donnees a caractere personnel dans le cadre du Service. Il annule et remplace tout accord anterieur portant sur le meme objet.

13.2. **Modification** -- Toute modification du present contrat doit faire l'objet d'un avenant ecrit signe par les deux Parties.

13.3. **Nullite partielle** -- Si l'une quelconque des dispositions du present contrat est declaree nulle ou inapplicable, les autres dispositions resteront en vigueur, et les Parties negocieront de bonne foi une disposition de remplacement.

13.4. **Notification** -- Toute notification au titre du present contrat doit etre adressee par ecrit (courrier recommande avec accuse de reception ou courrier electronique avec accuse de reception) aux adresses indiquees en tete du present contrat.

Fait en deux exemplaires originaux, a [A COMPLETER -- ville], le [A COMPLETER -- date].

Pour le Sous-traitant	**Pour le Responsable de traitement**
[A COMPLETER -- Nom et qualite]	[A COMPLETER -- Nom et qualite]
Signature :	Signature :

ANNEXE 1 -- DESCRIPTION DU TRAITEMENT

1. Nature des operations de traitement

Le Sous-traitant effectue pour le compte du Responsable de traitement les operations de traitement suivantes :

- Collecte et enregistrement des donnees a caractere personnel transmises par les personnes exercant leurs droits RGPD via le portail public ou saisies par le Responsable de traitement dans la Plateforme ;
- Conservation securisee des donnees dans une infrastructure chiffree hebergee en Union europeenne ;
- Organisation et structuration des donnees (registre des traitements, cartographie des sous-traitants, suivi des violations) ;
- Extraction et recherche automatisee de donnees dans les systemes tiers (data discovery) dans le cadre du traitement des demandes d'exercice de droits ;
- Consultation et analyse des donnees par des outils d'intelligence artificielle (Mistral AI) pour l'anonymisation, l'agregation et la generation de documents, dans les strictes limites des instructions du Responsable de traitement ;
- Communication par transmission des donnees (envoi d'emails transactionnels, reponses aux demandeurs, notifications) ;

- Mise a disposition des donnees au Responsable de traitement via la Plateforme ;
- Suppression des donnees conformement aux regles de retention et aux instructions du Responsable de traitement.

2. Finalite(s) du traitement

Le traitement a pour finalite la fourniture du service Garante, et notamment :

a) le traitement des demandes d'exercice de droits (DSAR) pour le compte des Clients du Cabinet ;

b) la tenue du registre des activites de traitement des Clients du Cabinet ;

c) la gestion et l'audit des sous-traitants des Clients du Cabinet ;

d) la gestion des violations de donnees des Clients du Cabinet ;

e) la generation de documents de conformite RGPD ;

f) l'envoi de communications transactionnelles (accuses de reception, notifications, reponses DSAR) ;

g) la production de rapports de conformite mensuels.

3. Types de donnees a caractere personnel traitees

Categorie	Donnees
Identite des demandeurs DSAR	Nom, prenom, adresse email, numero de telephone, adresse postale
Pieces d'identite	Copie de carte nationale d'identite ou de passeport (conservees 30 jours maximum)
Donnees collectees lors du data discovery	Toute donnee personnelle retrouvee dans les systemes des Clients du Cabinet (identite, coordonnees, donnees financieres, donnees comportementales, donnees RH, etc.)
Donnees du registre des traitements	Fiches de traitement Article 30 (metadonnees, pas de donnees personnelles directes)
Donnees des sous-traitants	Nom, coordonnees du contact, email, scores de conformite

Donnees des violations	Description de l'incident, categories de donnees affectees, nombre de personnes concernees
Donnees des comptes utilisateurs	Nom, adresse email, role, mot de passe (hache bcrypt), secret TOTP (chiffre AES-256-GCM)
Donnees techniques	Adresses IP, user-agent, horodatages d'actions, logs d'audit
Donnees de communication	Adresse email du destinataire, objet, statut de l'email, horodatages d'ouverture/clic

4. Categories de personnes concernees

- Personnes physiques exercant leurs droits RGPD aupres des Clients du Cabinet (demandeurs DSAR) ;
- Contacts chez les sous-traitants des Clients du Cabinet ;
- Personnes physiques concernees par une violation de donnees ;
- Utilisateurs de la Plateforme Garante (DPO, assistants, administrateurs du Cabinet).

5. Duree du traitement

Le traitement est effectue pendant toute la duree du Contrat Principal d'abonnement. Les durees de conservation specifiques sont les suivantes :

Categorie de donnees	Duree de conservation
Pieces d'identite (upload)	30 jours maximum apres verification, puis suppression automatique
Dossiers DSAR (donnees demandeur, reponses, audit)	Duree du contrat + 5 ans d'archivage (prescription)
Registre des traitements	Duree du contrat
Donnees sous-traitants	Duree du contrat
Donnees violations	Duree du contrat + 5 ans

Comptes utilisateurs	Duree du compte + 2 ans apres suppression
Logs techniques	12 mois glissants
Logs emails	12 mois glissants

ANNEXE 2 -- LISTE DES SOUS-TRAITANTS ULTERIEURS AUTORISES

Le Responsable de traitement autorise le recours aux sous-traitants ulterieurs suivants a la date de signature du present contrat :

Sous-traitant	Siege social	Service fourni	Localisation des donnees	DPA signe	Certifications / Garanties
Mistral AI SAS	Paris, France	Intelligence artificielle (LLM) : analyse des donnees DSAR, detection de donnees de tiers a anonymiser, generation de documents de conformite	France (UE)	Oui	Zero Data Retention (ZDR) active -- les donnees ne sont ni conservees ni utilisees pour l'entrainement du modele

Hetzner Online GmbH	Gunzenhausen, Allemagne	Hebergement de l'infrastructure (serveur dedie, base de donnees, stockage)	Allemagne (UE)	Oui	ISO 27001, SOC 1 Type II, SOC 2 Type II
Brevo (Sendinblue SAS)	Paris, France	Envoi d'emails transactionnels (accuses de reception, notifications, reponses DSAR)	France (UE)	Oui	Donnees traitees exclusivement dans l'UE
BunnyWay d.o.o. (Bunny.net)	Medvode, Slovenie	CDN, WAF (protection DDoS / OWASP Core Rule Set) et resolution DNS pour le domaine garante.fr ; donnees traitees : adresses IP des visiteurs, headers HTTP, cookies de session, logs d'acces	Slovenie + noeuds CDN UE	Oui	Donnees traitees exclusivement dans l'UE, Bunny Shield WAF actif

Conformement a l'Article 4.4 du present contrat, toute modification de cette liste sera notifiee au Responsable de traitement au moins trente (30) jours calendaires avant sa mise en oeuvre.

ANNEXE 3 -- MESURES TECHNIQUES ET ORGANISATIONNELLES

Les mesures techniques et organisationnelles mises en oeuvre par le Sous-traitant conformement a l'article 32 du RGPD sont les suivantes :

1. Chiffrement

Perimetre	Mesure
Donnees en transit	TLS 1.2/1.3 (reverse proxy Nginx), HSTS active (max-age=63072000)
Donnees au repos (stockage fichiers)	MinIO avec chiffrement cote serveur (SSE) AES-256-GCM
Donnees au repos (secrets applicatifs)	Chiffrement AES-256-GCM des tokens OAuth, mots de passe SMTP, secrets TOTP
Sauvegardes	Chiffrement AES-256-CBC (OpenSSL PBKDF2 100 000 iterations)
Mots de passe utilisateurs	Hachage bcrypt (12 rounds) avec politique de complexite (Zod)

2. Controle d'acces

Mesure	Detail
Multi-tenancy	Isolation stricte par identifiant de cabinet (cabinet_id) sur chaque requete API
Gestion des roles	Quatre roles : administrateur, DPO, assistant, lecture seule client
Authentification	JSON Web Token (acces : 15 minutes, rafraichissement : 7 jours), cookies HttpOnly SameSite=Strict

Authentification forte	2FA TOTP optionnel (recommande pour administrateurs)
Limitation des tentatives	5 requetes par 15 minutes par adresse IP sur l'authentification
Portail public	5 requetes par heure par adresse IP, champ honeypot anti-bot

3. Integrite et disponibilite

Mesure	Detail
Sauvegardes	pg_dump quotidien + volumes MinIO, chiffrees, retention 30 jours
Restauration	Script de restauration teste (scripts/restore.sh)
Conteneurisation	Docker Compose, 7 services isoles
Resilience	Redis en mode fail-open (indisponibilite Redis n'empeche pas le fonctionnement)

4. Tracabilite et audit

Mesure	Detail
Audit DSAR	Table dsar_audit_log : chaque action sur une demande de droits est journalisee (acteur, action, IP, horodatage)
Audit secrets	Table vault_audit_log : chaque acces aux secrets est journalise (cle accedee, jamais la valeur)
Audit IA	Table ai_audit_log : chaque appel a Mistral AI est journalise (fonction, prompt, reponse, latence, tokens)

Logs HTTP	Hook onResponse Fastify, logs structures JSON (Pino), masquage des parametres sensibles
Logs email	Table email_logs : suivi statut, ouverture, clic

5. Validation des entrees et protection contre les injections

Mesure	Detail
Validation	Schemas Zod sur chaque entree API
Requetes base de donnees	Prisma ORM avec requetes parametrees (pas de SQL brut)
Sanitisation	Interdiction de HTML dans les champs texte
CORS	Restreint au domaine de production, jamais wildcard (*)

6. Gestion des secrets

Mesure	Detail
Vault	Infisical (self-hosted, eu.infisical.com)
Rotation	Rafraichissement automatique toutes les 5 minutes (cron)
Audit	Journalisation de chaque acces (VaultAuditLog)
Variables d'amorce	Fichier .env (exclut du depot git), secrets applicatifs dans Infisical

7. Gestion des pieces d'identite

Mesure	Detail

Stockage	MinIO chiffre, structure /{cabinetId}/{clientId}/dsar/{dsarId}/identity/
Retention	30 jours maximum, suppression automatique par tache planifiee quotidienne
Formats acceptes	JPEG, PNG, PDF uniquement
Taille maximale	10 Mo

8. Mesures organisationnelles

Mesure	Detail
Politique de mots de passe	Complexite imposee par schema Zod (majuscule, minuscule, chiffre, caractere special, 8 caracteres minimum)
Principe du moindre privilege	Acces aux donnees limite selon le role de l'utilisateur
Separation des environnements	Developpement, preprod et production separes
Gestion des incidents	Procedure de notification des violations documentee (Annexe 5)

ANNEXE 4 -- INSTRUCTIONS DOCUMENTEES DU RESPONSABLE DE TRAITEMENT

Le Responsable de traitement donne au Sous-traitant les instructions suivantes :

Traiter les Donnees personnelles uniquement dans le cadre de la fourniture du Service Garante, tel que decrit a l'Annexe 1.

Heberger les Donnees personnelles exclusivement dans l'Union europeenne, sur l'infrastructure Hetzner (Allemagne), les services Mistral AI et Brevo (France) et Bunny.net (Slovenie, UE).

Appliquer les mesures de securite decrites a l'Annexe 3.

Supprimer automatiquement les pieces d'identite dans un delai de trente (30) jours apres la verification d'identite.

Notifier toute violation de donnees dans un delai maximum de quarante-huit (48) heures conformement a l'Article 4.7.

Ne pas utiliser les Donnees personnelles pour l'entrainement de modeles d'intelligence artificielle. L'option Zero Data Retention (ZDR) doit etre activee sur les services d'IA utilises.

Isoler strictement les donnees de chaque cabinet par le mecanisme de multi-tenancy (cabinet_id).

Conserver les dossiers DSAR pendant cinq (5) ans apres cloture, les logs techniques pendant douze (12) mois.

Cooperer avec le Responsable de traitement en cas de controle par la CNIL ou toute autre autorite de controle competente.

Appliquer le principe de minimisation : ne collecter et ne traiter que les Donnees personnelles strictement necessaires a la finalite de chaque traitement.

Toute instruction supplementaire sera communiquee par ecrit par le Responsable de traitement au Sous-traitant.

ANNEXE 5 -- PROCEDURE DE NOTIFICATION DES VIOLATIONS

1. Detection

Le Sous-traitant met en oeuvre des mecanismes de detection des violations de donnees, et notamment :
- Journalisation de toutes les actions sur les donnees (logs d'audit) ;
- Surveillance des acces non autorises ;
- Alertes automatiques en cas d'anomalie de securite.

2. Qualification

Des la detection d'un incident, le Sous-traitant procede a une evaluation initiale afin de determiner si l'incident constitue une violation de donnees a caractere personnel au sens de l'article 4(12) du RGPD.

3. Notification au Responsable de traitement

En cas de violation confirmee ou fortement suspectee, le Sous-traitant notifie le Responsable de traitement dans un delai maximum de **quarante-huit (48) heures** conformement a l'Article 4.7 du present

contrat.

La notification contient les elements enumeres a l'Article 4.7.2.

4. Notification a la CNIL et aux personnes concernees

La responsabilite de notifier la violation a la CNIL (article 33 du RGPD, delai de 72 heures) et, le cas echeant, aux personnes concernees (article 34 du RGPD) incombe au Responsable de traitement.

Le Sous-traitant assiste le Responsable de traitement dans l'accomplissement de ces obligations, en fournissant toutes les informations necessaires et en cooperant de bonne foi.

5. Mesures correctives

Le Sous-traitant met en oeuvre dans les meilleurs delais les mesures correctives necessaires pour :
- Contenir la violation et en limiter les consequences ;
- Identifier la cause de l'incident ;
- Prevenir la recurrence d'incidents similaires.

6. Documentation

Le Sous-traitant documente l'integralite de l'incident dans un registre dedie, comprenant :
- La chronologie des evenements ;
- La nature et l'etendue de la violation ;
- Les mesures prises et leur efficacite ;
- Les communications effectuees.

Cette documentation est conservee pendant une duree de cinq (5) ans et est mise a la disposition du Responsable de traitement et de l'autorite de controle sur demande.

Fin du contrat de sous-traitance de donnees a caractere personnel.