NOTE DE STRUCTURATION

Ce document est scindé en deux :

Sujet	Document
Politique de confidentialité (information des personnes, finalités, bases légales, durées, droits, cookies, sécurité, violation)	`covenant-confidentialite.md`
Accord de sous-traitance RGPD (art. 28) (relation Client responsable de traitement ↔ OWL sous-traitant)	**Le présent document**
Politique cookies (détail des traceurs)	`covenant-cookies.md`

Raison de la scission : la politique de confidentialité est un document public (page `/confidentialite`), tandis que l'accord de sous-traitance est un document contractuel (annexé aux contrats et devis). Les mélanger dans un même fichier créait de la confusion et des doublons avec `covenant-confidentialite.md`.

Conséquence pratique : - Pour toute question sur **ce que OWL fait des données** (finalités, durées, droits) → consulter `covenant-confidentialite.md`. - Pour toute question sur **la relation contractuelle Client ↔ OWL en matière de données** (rôles, obligations, sous-traitants ultérieurs, audit, sort des données) → consulter le présent document.

PARTIE 1 — ACCORD DE SOUS-TRAITANCE RGPD (ARTICLE 28)

> ***Ce document est contractuel.*** *Il est annexé aux contrats et devis lorsque la prestation implique un traitement de données personnelles pour le compte du Client (monitoring, infogérance, audits, interventions).* ***Il ne se substitue pas aux CGV.*** *En cas de contradiction, les CGV prévalent sur l'accord de sous-traitance, sauf disposition contraire expresse.* ***Il ne se substitue pas à la politique de confidentialité.*** *Celle-ci informe les personnes concernées (visiteurs, prospects, clients, salariés) sur les traitements réalisés par OWL SYSTEMS® pour son propre compte.*

---

1. OBJET DE L'ACCORD

Le présent accord est conclu entre :

- **Le Responsable de traitement** : le Client d'OWL SYSTEMS®, qui confie à OWL SYSTEMS® des prestations impliquant le traitement de données personnelles.
- **Le Sous-traitant** : OWL SYSTEMS®, qui traite les données pour le compte du Client.

Il est conclu en application de l'**article 28 du RGPD** et s'applique à toute prestation impliquant un traitement de données personnelles pour le compte du Client, notamment :

- Monitoring de site ou de serveur ;
- Infogérance de serveur ou de WordPress ;
- Audits de sécurité (site, serveur, WordPress, RGAA, SEO) ;
- Hardening et interventions ponctuelles ;
- Nettoyage post-attaque ;
- Onboarding.

Ne sont pas concernées les prestations qui n'impliquent aucun traitement de données personnelles pour le compte du Client (ex : formation inter-entreprises, audit RGAA sur données publiques).

L'astreinte, lorsqu'elle est acceptée, est assurée en interne par OWL SYSTEMS® et couverte par le présent accord. Aucun sous-traitant ultérieur n'intervient pour l'astreinte.

---

2. DESCRIPTION DU TRAITEMENT

Champ	Valeur
Nature du traitement	Supervision, infogérance, audits, hardening, interventions sur les serveurs web et sites du Client
Finalité	Exécution des prestations commandées
Catégories de personnes concernées	Visiteurs du site du Client, clients du Client, prospects du Client, salariés du Client
Catégories de données	Logs de connexion, adresses IP, données de formulaire, données de base de données, cookies, données de compte
Durée du traitement	Durée du contrat de prestation

Le Client est seul responsable de la licéité du traitement (base légale, information des personnes, consentement). OWL SYSTEMS® exécute les instructions du Client.

---

3. OBLIGATIONS D'OWL SYSTEMS® (SOUS-TRAITANT)

OWL SYSTEMS® s'engage à :

1. **Traiter les données uniquement sur instruction documentée du Client**, y compris pour les transferts vers un pays tiers. Si OWL SYSTEMS® considère qu'une instruction constitue une violation du RGPD, elle en informe immédiatement le Client.
2. **Garantir la confidentialité** des données traitées (voir `covenant-cgu-cgv.md` §10).
3. **Mettre en œuvre les mesures de sécurité** décrites au §7.
4. **Ne pas faire appel à un sous-traitant ultérieur** sans autorisation écrite préalable du Client (voir §5).
5. **Aider le Client** à répondre aux demandes d'exercice des droits des personnes concernées (accès, rectification, effacement, limitation, opposition, portabilité).
6. **Aider le Client** à respecter ses obligations en matière de sécurité, de notification des violations et d'analyse d'impact (AIPD).
7. **Supprimer ou restituer les données** à la fin du contrat, au choix du Client (voir §10).
8. **Mettre à disposition** les informations nécessaires pour démontrer le respect de l'article 28 (voir §11).

9. **Notifier au Client** toute violation de données personnelles dans les **48 heures** suivant la prise de connaissance (délai contractuel plus court que le délai légal de 72 h, pour permettre au Client de notifier la CNIL dans les temps — voir §9).
10. **Former et sensibiliser** son personnel à la protection des données.
11. **Tenir un registre** des catégories d'activités de traitement effectuées pour le compte du Client (art. 30.2 RGPD).

---

4. OBLIGATIONS DU CLIENT (RESPONSABLE DE TRAITEMENT)

Le Client s'engage à :

1. **Documenter par écrit** toute instruction concernant les traitements confiés à OWL SYSTEMS®.
2. **Veiller, au préalable et pendant toute la durée** de chaque traitement, au respect des obligations prévues par le RGPD.
3. **Superviser le traitement**, y compris réaliser les audits et les inspections auprès du sous-traitant (voir §11).
4. **Exploiter les éventuelles données transmises** en exécution de la Prestation conformément au RGPD et à la réglementation applicable au Contrat.
5. **Garantir OWL SYSTEMS®** contre toute action, de quelque nature qu'elle soit, pouvant être intentée contre lui par une personne concernée ou tout tiers pour non-respect par le Client, directement ou indirectement du fait de ses demandes et instructions à OWL SYSTEMS®, de la réglementation applicable en matière de protection des données à caractère personnel.

---

5. SOUS-TRAITANTS ULTÉRIEURS

Le Client autorise OWL SYSTEMS® à faire appel aux **sous-traitants ultérieurs** listés ci-dessous.

5.1 Liste des sous-traitants ultérieurs

Sous-traitant	Service	Siège	Données traitées	Garanties
OVH SAS	Hébergement infrastructure	France (UE)	Sites, mails, logs, sauvegardes	Aucun transfert hors UE pour les données client final
Scaleway	Hébergement (Dedibox / VPS)	France (UE)	Sites, mails, logs, sauvegardes (données client final)	Aucun transfert hors UE
TierHive	Hébergement (VPS)	France (UE)	Sites, mails, logs, sauvegardes (données client final)	Aucun transfert hors UE
DediRock	VPS techniques (bastion, VPN, CA, backup, cloud interne) **et gateway mail**	États-Unis	**Aucune donnée personnelle au repos.** Le gateway mail (smarthost) traite des données personnelles **en transit** (soumissions de formulaires : nom, email, message) sans stockage durable, avec relais immédiat vers l'infrastructure de réception UE. Les services techniques (bastion, VPN, CA, backup, cloud interne) ne traitent aucune donnée personnelle.	CCT signées et analyse de transfert documentée.
RackNerd	Hébergement VPS techniques	États-Unis	**Aucune donnée personnelle** (services techniques : bastion, VPN, CI, backup)	Documentation interne de l'absence de données personnelles ; si des données person-

Sous-traitant	Service	Siège	Données traitées	Garanties
				nelles venaient à être traitées, CCT et analyse de transfert seraient mises en place avant tout traitement
Sonia Andros (SEO)	Prestation SEO (audit, mise en place)	France (UE)	Données de navigation (Search Console, Analytics), données publiques du site	Aucun transfert hors UE. **Intervient sous la responsabilité d'OWL SYSTEMS® dans le cadre des prestations SEO sous-traitées.**
Shine	Services bancaires et facturation électronique (plateforme agréée)	France (UE)	Coordonnées bancaires, données de facturation	Aucun transfert hors UE. **Shine n'intervient pas sur les serveurs du Client.**
Stripe	Paiement en ligne (prévu, non actif à ce jour)	Irlande (UE) / États-Unis	Données de paiement	**PCI-DSS. CCT signées (réf. à archiver) ; analyse de transfert documentée.**
PayPal	Paiement en ligne (prévu, non actif à ce jour)	Luxembourg (UE)	Données de paiement	**PCI-DSS. Aucun transfert hors UE.**

Shine est un prestataire de services bancaires et de facturation électronique, pas un sous-traitant technique intervenant sur les serveurs du Client. Il est mentionné pour transparence, mais son rôle diffère de celui d'OVH, Scaleway ou Stripe.

L'astreinte, lorsqu'elle est acceptée, est assurée en interne par OWL SYSTEMS® : aucun sous-traitant ultérieur n'intervient pour cette prestation.

Les prestataires de support d'OWL SYSTEMS® (IONOS, OpenProvider, TryHackMe) ne traitent pas de données personnelles pour le compte des clients. Ils ne figurent donc pas dans la présente liste.

5.2 Modalités de modification

Tout ajout ou remplacement d'un sous-traitant ultérieur au sens du RGPD est notifié au Client 30 jours avant sa mise en œuvre. Le Client peut s'y opposer pour motif légitime. En cas de désaccord persistant, le Client peut résilier le contrat sans pénalité.

Les sous-traitants ultérieurs sont soumis aux **mêmes obligations** que celles du présent accord, notamment en matière de confidentialité et de sécurité.

---

6. TRANSFERTS HORS UNION EUROPÉENNE

Les transferts hors UE sont encadrés par les **Clauses Contractuelles Types (CCT)** de la Commission européenne, ou par tout autre mécanisme légal approprié (décision d'adéquation, règles d'entreprise contraignantes).

Les VPS hébergés chez DediRock (États-Unis) n'hébergent **aucune donnée personnelle au repos**. Ils hébergent des services techniques utilisés par OWL SYSTEMS® pour son propre fonctionnement (bastion, VPN, CA, backup, cloud interne). Le gateway mail hébergé chez DediRock traite des données personnelles **en transit** (soumissions de formulaires) **sans stockage durable** : les emails sont relayés immédiatement vers l'infrastructure de réception située dans l'Union européenne. Les CCT sont signées et l'analyse de transfert est documentée. Les données clients (sites, mails, logs au repos) sont hébergées dans l'Union européenne.

Stripe traite des données de paiement (lorsqu'il sera activé). OWL SYSTEMS® a signé les CCT et documenté l'analyse de transfert. En attendant l'activation, aucune donnée de paiement n'est traitée par OWL SYSTEMS®.

PayPal traite des données de paiement (lorsqu'il sera activé). PayPal est basé au Luxembourg (UE) : aucun transfert hors UE.

---

7. MESURES DE SÉCURITÉ

OWL SYSTEMS® met en œuvre les mesures techniques et organisationnelles suivantes :

Mesure	Détail
Chiffrement en transit	HTTPS obligatoire, TLS 1.2+
Chiffrement des sauvegardes	Sauvegardes Restic chiffrées
Gestion des secrets	Vaultwarden (auto-hébergé), KeePassXC
Authentification	Mots de passe forts, 2FA activée partout où possible
Séparation des privilèges	Comptes distincts par usage
Journalisation	Logs centralisés, conservation 30 jours à 12 mois selon la nature
Sauvegardes	Restic quotidien, rétention 1 semaine / 1 mois / 3 mois
Tests de restauration	**Tests mensuels sur un échantillon représentatif ; restauration complète testée annuellement. Ces tests ne garantissent pas la restauration de l'intégralité des données en cas d'incident majeur.**
Hardening	SSH, firewall, Fail2ban, mises à jour régulières
Accès physique	Hébergement dans l'Union européenne, pas d'accès physique d'OWL SYSTEMS®

Le chiffrement au repos porte sur les sauvegardes. Les volumes de production ne sont pas nécessairement chiffrés au repos.

Aucune certification ISO 27001, HDS ou SOC 2 n'est détenue à ce jour. OWL SYSTEMS® ne prétend pas être conforme à ces référentiels. Les mesures ci-dessus sont mises en œuvre de bonne foi, dans une logique d'obligation de moyens.

---

8. DROITS DES PERSONNES CONCERNÉES

OWL SYSTEMS® aide le Client à répondre aux demandes d'exercice des droits :

- **Accès** : fourniture des logs et données traitées.
- **Rectification** : correction des données inexactes.
- **Effacement** : suppression des données, sous réserve des obligations légales de conservation.

- **Limitation** : suspension du traitement.
- **Opposition** : suspension du traitement pour motif légitime. **En matière de prospection directe, l'opposition peut être exercée à tout moment, sans motif.**
- **Portabilité** : export des données dans un format structuré, couramment utilisé et lisible par machine.

Les demandes sont adressées à `rgpd@owl-systems.com` et traitées dans un délai d'un (1) mois, prolongeable de deux (2) mois en cas de complexité ou de nombre important de demandes.

OWL SYSTEMS® adresse sans délai toute demande qui serait formulée auprès de lui au Client, et n'est pas tenu d'y répondre directement.

---

9. NOTIFICATION DES VIOLATIONS

En cas de violation de données personnelles, OWL SYSTEMS® notifie au Client :

- **La nature de la violation** (catégories et nombre approximatif de personnes concernées, catégories et nombre approximatif d'enregistrements concernés) ;
- **Les conséquences probables** de la violation ;
- **Les mesures prises ou envisagées** pour remédier à la violation et en atténuer les effets ;
- **Le nom et les coordonnées** du point de contact.

La notification est faite dans les 48 heures suivant la prise de connaissance. Si les informations ne sont pas toutes disponibles, elles sont fournies par étapes successives.

Contact pour signaler une violation : `security@owl-systems.com`.

---

10. ANALYSE D'IMPACT (AIPD)

OWL SYSTEMS® aide le Client, sur demande, à réaliser une **analyse d'impact relative à la protection des données** (art. 35 du RGPD), en fournissant :

- La description des traitements effectués ;
- Les mesures de sécurité mises en place ;
- Les risques identifiés ;
- Les mesures d'atténuation.

Cette aide est fournie dans le cadre de la prestation. Elle ne se substitue pas à l'AIPD que le Client reste seul responsable de réaliser et de documenter.

11. AUDIT

Le Client peut auditer OWL SYSTEMS® **une fois par an**, sur préavis de **30 jours**, pour vérifier le respect du présent accord. L'audit est réalisé :

- À distance, sur pièces (documentation, logs, procédures) ;
- Sur site, si nécessaire, dans les locaux d'OWL SYSTEMS® ;
- Par le Client ou un tiers mandaté, soumis à des obligations de confidentialité.

L'audit est **pris en charge par le Client**. Il ne peut pas perturber le fonctionnement d'OWL SYSTEMS® ou de ses autres clients.

OWL SYSTEMS® tient à la disposition du Client la documentation nécessaire pour démontrer le respect de toutes ses obligations (registre des activités de traitement, procédures, mesures de sécurité).

---

12. SORT DES DONNÉES EN FIN DE CONTRAT

À la fin du contrat, OWL SYSTEMS® :

1. **Révoque les accès** (clés SSH, comptes dédiés) ;
2. **Documente et restitue gratuitement** au Client les éléments nécessaires à la continuité (configurations, scripts, playbooks) ;
3. **Supprime les secrets et identifiants** (clés SSH, tokens, mots de passe) ;
4. **Supprime ou anonymise les configurations contenant des données personnelles** ;
5. **Peut conserver des données techniques anonymisées** (journaux agrégés, métriques) pour la maintenance et les statistiques, pour une durée maximale de **douze (12) mois**, sur la base de son intérêt légitime ;
6. **Atteste par écrit** la suppression des secrets et configurations au Client, sur demande.

OWL SYSTEMS® n'étant pas hébergeur, les données du Client restent en permanence sur les serveurs du Client, chez son hébergeur. La restitution porte sur les configurations, scripts, playbooks et rapports produits par OWL SYSTEMS®.

La restitution des éléments nécessaires à la continuité est gratuite. Une prestation d'accompagnement supplémentaire (migration, formation d'un tiers, audit de reprise) peut être facturée au tarif de l'intervention ponctuelle ou selon devis. **La restitution des éléments nécessaires à la continuité ne peut être refusée pour quelque motif que ce soit, y compris en cas de litige financier.**

---

13. RESPONSABILITÉ

OWL SYSTEMS® est responsable des dommages causés par le traitement **si elle n'a pas respecté les obligations du RGPD qui incombent spécifiquement aux sous-traitants** (art. 82.2 du RGPD).

Le Client reste responsable :

- De la licéité du traitement ;
- De l'information des personnes concernées ;
- Du recueil du consentement lorsque nécessaire ;
- De la conformité de son site et de son infrastructure aux obligations légales.

---

14. DURÉE

Le présent accord est conclu pour la **durée du contrat de prestation**. Il prend fin automatiquement à la fin du contrat, sous réserve des obligations qui survivent (confidentialité, conservation légale, responsabilité).

---

15. DROIT APPLICABLE ET JURIDICTION

Le présent accord est soumis au **droit français**. Tout litige relève de la compétence exclusive du **Tribunal de commerce de Melun**, conformément aux CGV, **sous réserve que le Client ait la qualité de commerçant au sens du droit français et que les conditions de l'article 48 du Code de procédure civile soient remplies. À défaut, les juridictions de droit commun seront compétentes.**