ZORROOO - Infrastructure ODR

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

Document de référence RGPD - Version 1.0 - Janvier 2026
Responsable de traitement : ZORROOO SAS (RCS Nancy 983 661 851)

RÉSUMÉ EXÉCUTIF

Contexte

Zorrooo opère une infrastructure technique neutre de résolution en ligne de litiges (ODR) mettant en relation citoyens et professionnels du droit. En tant qu'hébergeur au sens de la LCEN 2004, Zorrooo traite des données personnelles dans le cadre des litiges soumis par les utilisateurs.

Conclusion de l'AIPD

Le traitement présente des risques maîtrisés grâce à :

- Architecture technique "privacy by design"
- Mesures de sécurité renforcées (chiffrement, hébergement France)
- Séparation stricte des espaces (public/privé)
- Mécanismes de contrôle utilisateur sur leurs données

Les mesures mises en œuvre ramènent tous les risques à un niveau acceptable.

PARTIE 1 : DESCRIPTION SYSTÉMATIQUE DU TRAITEMENT

1.1 Nature et finalités du traitement

Infrastructure technique ODR

Finalité principale : Mise à disposition d'outils techniques permettant :

1. Hébergement de contenus publiés par les utilisateurs relatifs à leurs litiges
2. Mise en relation technique entre citoyens et professionnels du droit
3. Communication sécurisée (forum public + messagerie privée)
4. Facilitation du paiement via prestataire tiers agréé ACPR (Stripe)

Base légale : Exécution du contrat (Art. 6.1.b RGPD)

Traitements complémentaires

1. **Information générale** (Art. 6.1.f RGPD - intérêt légitime) :
   Fourniture d'informations non personnalisées, orientation vers professionnels habilités

2. **Amélioration du service** (Art. 6.1.f) :
   Analyses statistiques agrégées, optimisation technique

3. **Conformité réglementaire** (Art. 6.1.c - obligation légale) :
   Conservation preuves (LCEN), réponse aux réquisitions

1.2 Données traitées

1.2.1 Données d'identification (Citoyens)

Données collectées :

- Identité : nom, prénom, sexe, date de naissance
- Contact : email, téléphone
- Localisation : adresse postale, code postal, ville

Justification :

- Identification nécessaire pour gestion compte (Art. 6.1.b)
- Communication sur statut réclamations (Art. 6.1.b)
- Prévention fraude/abus (Art. 6.1.f)

Minimisation : Aucune donnée administrative (CNI, IBAN) collectée sauf nécessité justifiée

1.2.2 Données de litige

Données collectées :

- Description factuelle du litige (texte libre)
- Documents justificatifs (factures, bons de commande, échanges emails, photos)
- Montant du préjudice estimé
- Coordonnées de l'entreprise mise en cause
- Historique des échanges

Justification :

- Traitement du litige (Art. 6.1.b)
- Mise en relation avec professionnels compétents (Art. 6.1.b)
- Conservation preuve (Art. 6.1.c)

Risque identifié : Données sensibles (Art. 9 RGPD) possibles dans descriptions libres **Mesure** : Avertissement explicite + détection automatique patterns sensibles

1.2.3 Données professionnels du droit

Données collectées :

- Identité : nom, prénom, structure
- Qualifications : inscription barreau, certifications
- Contact : email professionnel, téléphone
- Domaines d'expertise (299 compétences cartographiées)
- Historique interventions (statistiques anonymisées)

Justification :

- Vérification habilitations professionnelles (Art. 6.1.c)
- Matching avec litiges (Art. 6.1.b)
- Transparence pour citoyens (Art. 6.1.f)

1.2.4 Données techniques

Données collectées :

- Logs connexion (IP, user-agent, timestamps)
- Données de navigation (pages vues, durée sessions)
- Cookies techniques et analytiques
- Événements applicatifs (actions utilisateurs)

Justification :

- Sécurité/détection fraudes (Art. 6.1.f)
- Performance technique (Art. 6.1.f)
- Conformité LCEN (Art. 6.1.c - conservation 12 mois)

Minimisation : IP masquées après 24h sauf nécessité sécurité

1.2.5 Données sensibles (Art. 9 RGPD)

Principe : Aucune collecte systématique.

Cas d'occurrence : Divulgation volontaire par l'utilisateur dans description du litige (santé, origines ethniques, opinions politiques, vie sexuelle).

Base légale : Consentement explicite (Art. 9.2.a RGPD) ou défense droits en justice (Art. 9.2.f).

Mesures de protection :

1. Avertissement explicite lors dépôt litige
2. Détection automatique patterns sensibles avec alerte utilisateur

3. Pseudonymisation renforcée pour analyses internes
4. Accès restreint avec logs d'accès renforcés

1.3 Personnes concernées

1.3.1 Citoyens/Plaignants

- **Profil** : Personnes physiques ≥16 ans, personnes morales
- **Volume** : 5 000+ utilisateurs actifs

Mesures de protection : Langue claire, droit d'effacement renforcé, support accessible

1.3.2 Professionnels du droit

- **Profil** : Avocats, structures Art.55, médiateurs, experts métiers
- **Volume** : 600+ professionnels actifs

Mesures spécifiques : Vérification habilitations, rappels obligations légales

1.3.3 Tiers mentionnés

- **Profil** : Entreprises mises en cause, témoins
- **Volume** : ~750 entreprises/an

Mesures spécifiques : Droit opposition renforcé, procédure signalement visible

1.4 Destinataires des données

1.4.1 Personnel Zorrooo

Personnel habilité (support technique, support utilisateurs, équipe sécurité) avec accès restreint selon principe du moindre privilège. Authentification forte obligatoire, logs d'accès audités.

1.4.2 Sous-traitants (Art. 28 RGPD)

Hébergement : OVH France (Roubaix + Gravelines)

- Certification ISO 27001, HDS
- Contrat DPA Art. 28 signé
- Aucun transfert hors UE

Paiement : Stripe (agréé ACPR)

- PCI-DSS niveau 1
- Transfert UE-US : Clauses contractuelles types Commission UE

Autres prestataires : Analytics (Plausible - Allemagne), Email (Brevo - France)

- Tous contrats DPA Art. 28 signés

- Hébergement UE
- Audits sécurité réguliers

1.4.3 Destinataires externes

Professionnels du droit : Accès données litige uniquement si le citoyen initie le contact privé

Autorités compétentes : Sur réquisition judiciaire ou obligation légale uniquement

Aucun partage commercial : Pas de revente données, pas de profilage publicitaire

1.5 Durées de conservation

Catégorie	Durée active	Archivage	Justification
Compte utilisateur	Pendant inscription	3 ans après clôture	Gestion contentieux
Données de litige	Traitement + 6 mois	3 ans	Prescription civile
Paiements	-	10 ans	Obligations comptables
Logs connexion	12 mois	-	Obligation LCEN
Cookies	13 mois max	-	Recommandation CNIL
Données anonymisées	Illimitée	-	Hors champ RGPD

1.6 Transferts hors UE

Principe : Aucun transfert systématique hors UE.

Exception encadrée : Stripe (traitement paiements) - États-Unis

- Garantie : Clauses contractuelles types Commission UE (2021)
- Mesures : Chiffrement données sensibles, évaluation transfert (TIA)

Transparence : Liste complète sous-traitants disponible sur demande.

PARTIE 2 : ÉVALUATION DE LA NÉCESSITÉ ET DE LA PROPORTIONNALITÉ

2.1 Nécessité du traitement

Finalités légitimes :

- Accès à la justice (objectif constitutionnel)
- Résolution alternative litiges (Directive 2013/11/UE, Règlement UE 524/2013)
- Désengorgement tribunaux (Loi Programmation Justice)

Solution retenue : Infrastructure centralisée avec minimisation données, séparation espaces public/privé, contrôle utilisateur renforcé.

2.2 Proportionnalité des données collectées

Minimisation appliquée - Données NON collectées :

- CNI/Passeport (sauf vérification professionnels)
- Coordonnées bancaires (gérées par Stripe uniquement)
- Historique navigation hors plateforme
- Géolocalisation précise

Données optionnelles : Photo profil, téléphone, adresse complète

2.3 Information des personnes

Transparence renforcée :

- Politique de confidentialité accessible (langage clair, version courte + complète)
- Information contextuelle lors dépôt litige et contact professionnel
- Bandeau cookies conforme CNIL
- Page dédiée "Vos droits RGPD"

2.4 Droits des personnes

Facilitation exercice droits :

Droit	Modalité
Accès (Art. 15)	Export automatisé (JSON + PDF)
Rectification (Art. 16)	Modification directe paramètres
Effacement (Art. 17)	Suppression < 48h
Limitation (Art. 18)	Gel traitement disponible
Portabilité (Art. 20)	Format structuré (JSON)
Opposition (Art. 21)	Formulaire dédié

Consentement (Art. 7)	Retrait aussi simple que donner

Délai de réponse : < 1 mois (RGPD)

PARTIE 3 : RISQUES POUR LES DROITS ET LIBERTÉS

3.1 Méthodologie d'évaluation

Échelle gravité : Négligeable | Limitée | Importante | Maximale
Échelle vraisemblance : Négligeable | Limitée | Importante | Maximale
Niveau de risque : Gravité × Vraisemblance

3.2 Risque 1 : Accès non autorisé aux données de litige

Description : Accès illégitime aux dossiers citoyens (piratage, insider threat).

Impact : Gravité MAXIMALE - Violation vie privée, préjudice moral, chantage, atteinte réputation
Vraisemblance : LIMITÉE (mesures en place)
Risque résiduel : ACCEPTABLE

Mesures techniques :

- Chiffrement TLS 1.3 (transit) + AES-256 (repos)
- Authentification MFA, autorisation RBAC
- Séparation bases données, cloisonnement réseau
- Logs accès audités mensuellement
- Pentests annuels, scans vulnérabilités hebdomadaires

Mesures organisationnelles :

- Formation personnel, sanctions disciplinaires
- Politique sécurité documentée, procédure incident
- Audit sous-traitants avant contractualisation

Infrastructure : Datacenters OVH (accès biométrique, surveillance 24/7, redondance géographique)

3.3 Risque 2 : Divulgation non consentie de données sensibles (Art. 9)

Description : Publication involontaire données sensibles (santé, origines, opinions) dans descriptions litiges.

Impact : Gravité MAXIMALE - Discrimination, stigmatisation, atteinte dignité
Vraisemblance : IMPORTANTE (divulgation volontaire fréquente)
Risque résiduel : ACCEPTABLE

Mesures préventives :

- Avertissement explicite lors dépôt litige (bandeau rouge)
- Détection automatique patterns sensibles (IA) avec alerte utilisateur
- Pseudonyme obligatoire forum public
- Documents justificatifs jamais publics
- Droit effacement renforcé

Mesures correctives :

- Bouton "Signaler" visible
- Traitement prioritaire < 24h
- Équipe modération 7j/7

3.4 Risque 3 : Usage détourné par professionnels

Description : Démarchage hors cadre, revente listes, prospection commerciale abusive.

Impact : Gravité IMPORTANTE - Spam, perte confiance, atteinte réputation
Vraisemblance : LIMITÉE
Risque résiduel : FAIBLE

Mesures contractuelles :

- Interdiction explicite CGS (clause pénale 10 000€)
- Charte éthique signée obligatoire

Mesures techniques :

- Accès données uniquement si citoyen initie contact
- Monitoring comportements suspects
- Watermarking invisible (traçabilité fuites)
- Historique conservé 3 ans

Mesures organisationnelles :

- Vérification qualifications manuelle
- Procédure signalement dédiée
- Transmission autorités si violation grave

3.5 Risque 4 : Réidentification données anonymisées

Description : Reconstitution identité via croisement données anonymisées.

Impact : Gravité IMPORTANTE - Violation vie privée, profilage non consenti
Vraisemblance : LIMITÉE
Risque résiduel : FAIBLE

Mesures techniques :

- Anonymisation robuste (conformité CNIL G29)
- K-anonymat minimum k=5
- Généralisation données, suppression combinaisons uniques
- Test ré-identification annuel externe
- Séparation environnements (interdiction re-jonction bases)

Mesures organisationnelles :

- Data scientists : accès anonymisées uniquement
- Revue DPO avant publication statistiques
- Interdiction publication < 10 individus

3.6 Risque 5 : Perte/destruction accidentelle données

Description : Perte définitive suite incident technique (crash, erreur humaine, sinistre).

Impact : Gravité IMPORTANTE - Perte preuve, impossibilité continuer traitement
Vraisemblance : LIMITÉE (infrastructure redondante)
Risque résiduel : FAIBLE

Mesures techniques :

- Sauvegardes automatisées (quotidiennes 7j, hebdo 4 sem, mensuelles 3 mois)
- Redondance infrastructure (RAID 10, réplication synchrone, multi-AZ)
- Monitoring temps réel, astreinte 24/7
- PRA documenté : RPO 24h, RTO 4h

Mesures organisationnelles :

- Formation équipe, procédures restauration testées annuellement
- Environnement staging, validation changements
- Post-mortem incidents

Mesures contractuelles : SLA OVH 99,9%, assurance cyber-risques

3.7 Risque 6 : Non-conformité traitement transfrontalier (Stripe)

Description : Transfert données vers États-Unis (Stripe) potentiellement non conforme.

Impact : Gravité IMPORTANTE - Surveillance US, atteinte souveraineté
Vraisemblance : LIMITÉE (mesures compensatoires)
Risque résiduel : ACCEPTABLE

Mesures juridiques :

- Clauses contractuelles types (CCT) Commission UE 2021
- Transfer Impact Assessment (TIA) réalisée, revue annuelle

Mesures techniques :

- Chiffrement renforcé bout-en-bout (AES-256 + RSA-4096)
- Pseudonymisation, dissociation données paiement/litige
- Minimisation volume transféré

Mesures organisationnelles :

- Veille juridique (CJUE), transparence utilisateurs
- Évaluation alternatives UE, roadmap prestataire UE 2027

3.8 Synthèse cartographie des risques

Risque	Gravité	Vraisemblance	Niveau Initial	Niveau Résiduel	Acceptabilité
Accès non autorisé	Maximale	Limitée	ÉLEVÉ	ACCEPTABLE	✓
Données sensibles Art. 9	Maximale	Importante	CRITIQUE	ACCEPTABLE	✓
Usage détourné pros	Importante	Limitée	MODÉRÉ	FAIBLE	✓
Réidentification	Importante	Limitée	MODÉRÉ	FAIBLE	✓
Perte données	Importante	Limitée	MODÉRÉ	FAIBLE	✓
Transfert Stripe	Importante	Limitée	MODÉRÉ	ACCEPTABLE	✓

Conclusion : Tous les risques identifiés présentent un niveau résiduel ACCEPTABLE ou FAIBLE grâce aux mesures mises en œuvre.

PARTIE 4 : MESURES ENVISAGÉES

4.1 Mesures techniques

Sécurité infrastructure :

- Chiffrement TLS 1.3 (transit) + AES-256 (repos)
- Authentification MFA, contrôles RBAC
- Journalisation + audit mensuel
- Pentests annuels, scans hebdomadaires
- WAF + anti-DDoS
- Sauvegardes automatisées 3-2-1
- Redondance multi-AZ

Protection données :

- Pseudonymisation environnements non-prod

- Anonymisation robuste (k-anonymat ≥5)
- Détection automatique données sensibles
- Séparation bases données
- Chiffrement bout-en-bout messagerie

Contrôle utilisateurs :

- Export données automatisé
- Suppression compte < 48h
- Gestion consentements granulaire
- Bandeau cookies conforme CNIL

4.2 Mesures organisationnelles

Gouvernance :

- DPO désigné
- Registre traitements à jour
- Politique sécurité documentée
- Procédure incident response
- Comité sécurité trimestriel

Formation :

- Onboarding sécurité obligatoire
- Rappels trimestriels
- Formation RGPD annuelle

Contractualisation :

- DPA Art. 28 tous sous-traitants
- Audit avant contractualisation
- Revue annuelle conformité

Conformité continue :

- Veille juridique RGPD
- Revue annuelle AIPD
- Tests conformité automatisés

4.3 Privacy by Design

Architecture :

- Minimisation par défaut
- Séparation espaces public/privé
- Pseudonymisation native forum
- Suppression facilitée

Fonctionnalités :

- Contrôle visibilité utilisateur

- Alerte données sensibles
- Historique actions consultable
- Export machine-readable

Paramètres par défaut :

- Profil privé (opt-in visibilité)
- Cookies strictement nécessaires
- Pas de tracking tiers
- Pseudonyme aléatoire généré

4.4 Transparence

- Politique confidentialité détaillée
- Charte cookies
- Page "Vos droits RGPD"
- Liste sous-traitants accessible
- Rapport transparence annuel

PARTIE 5 : VALIDATION ET SUIVI

5.1 Validation

Validation technique : CTPO - 15/01/2026
Validation juridique : Conseil externe - 18/01/2026
Validation DPO : 20/01/2026
Validation Direction : CEO - 22/01/2026

5.2 Consultation CNIL

Évaluation Art. 36 RGPD : Consultation CNIL obligatoire si risque élevé malgré mesures.

Conclusion : Pas de consultation CNIL nécessaire. Tous risques résiduels acceptables ou faibles.

5.3 Plan de suivi

Revue annuelle obligatoire : Janvier chaque année

Revue exceptionnelle si :

- Nouvelle finalité/catégorie données
- Nouveau sous-traitant critique
- Transfert nouveau pays tiers
- Incident sécurité majeur
- Décision CNIL/CJUE impactante

Indicateurs de suivi :

- Disponibilité infrastructure >99,9%
- Délai réponse droits <15j
- Incidents RGPD : objectif 0
- Taux détection données sensibles >90%

5.4 Responsabilités

DPO : Pilotage AIPD, conseil conformité, point de contact CNIL
CTPO : Implémentation mesures techniques, architecture sécurité
CEO : Validation stratégique, allocation ressources, responsabilité finale
Support : Traitement demandes droits, gestion signalements

5.5 Documentation associée

- Registre traitements (Art. 30 RGPD)
- Politique sécurité SI
- Procédure gestion violations données
- DPA sous-traitants
- TIA Stripe
- Politique cookies
- CGU/CGS/Politique confidentialité

CONCLUSION

Synthèse générale

Zorrooo a mis en œuvre une approche rigoureuse de protection des données :

- **Privacy by Design** : Architecture minimisant la collecte et maximisant le contrôle utilisateur
- **Sécurité renforcée** : Chiffrement, hébergement France, audits réguliers
- **Transparence** : Politique claire, droits facilités, rapport annuel
- **Conformité** : Contrats Art. 28, TIA documentée, registre à jour

Niveau de risque global

Tous les risques identifiés sont maîtrisés :

- Accès non autorisé : ACCEPTABLE
- Données sensibles Art. 9 : ACCEPTABLE
- Usage détourné pros : FAIBLE
- Réidentification : FAIBLE
- Perte données : FAIBLE
- Transfert Stripe : ACCEPTABLE

Consultation CNIL

Non nécessaire (Art. 36 RGPD) : Les mesures mises en œuvre ramènent tous les risques à un niveau acceptable.

Engagement amélioration continue

Zorrooo s'engage à :

- Revue annuelle systématique AIPD
- Mise à jour réactive si évolution traitement
- Investissement continu sécurité
- Veille réglementaire proactive

Document approuvé par :

- CEO Zorrooo SAS
- CTPO Zorrooo SAS
- DPO Zorrooo
- Conseil juridique externe

Date d'approbation : 22 janvier 2026
Prochaine revue : Janvier 2027 **Version** : 1.0