DATA PROTECTION IMPACT ASSESSMENT

ZORROOO - ODR Infrastructure

GDPR Reference Document

Version 1.0 - January 2026

Data Controller: ZORROOO SAS (RCS Nancy 983 661 851)

DPO Contact: support@zorr.ooo

EXECUTIVE SUMMARY

Context

Zorrooo operates a neutral technical infrastructure for online dispute resolution (ODR) connecting citizens with legal professionals. As a host under LCEN 2004, Zorrooo processes personal data in the context of disputes submitted by users.

DPIA Conclusion

The processing presents controlled risks thanks to:

- Privacy by design architecture
- Enhanced security measures (encryption, France hosting)
- Strict separation of spaces (public/private)
- User control mechanisms over their data

All implemented measures bring risks to an acceptable level.

PART 1: SYSTEMATIC DESCRIPTION OF PROCESSING

1.1 Nature and Purpose of Processing

ODR Technical Infrastructure

Main purpose: Provision of technical tools enabling:

1. Hosting content published by users regarding their disputes
2. Technical connection between citizens and legal professionals
3. Secure communication (public forum + private messaging)
4. Payment facilitation via third-party ACPR-approved provider (Stripe)

Legal basis: Contract execution (Art. 6.1.b GDPR)

Complementary Processing

1. **General information** (Art. 6.1.f GDPR - legitimate interest): Non-personalized information provision, guidance to authorized professionals
2. **Service improvement** (Art. 6.1.f): Aggregated statistical analyses, technical optimization
3. **Regulatory compliance** (Art. 6.1.c - legal obligation): Evidence retention (LCEN), requisition responses

1.2 Data Processed

Category	Data Collected	Justification
Identity (Citizens)	Name, first name, gender, date of birth, email, phone	Account management, fraud prevention
Dispute Data	Factual description, supporting documents, estimated damages, dispute type	Dispute processing, professional matching, evidence
Legal Professionals	Identity, qualifications (bar registration), professional email, specialization areas	Qualification verification, matching, transparency
Technical Data	Connection logs (IP, user-agent), navigation data, cookies	Security, fraud detection, technical performance
Sensitive Data (Art. 9)	Voluntary disclosure only (health, origins, opinions)	Explicit consent OR defense of rights

1.3 Data Subjects

- **Citizens/Complainants:** Individuals ≥16 years, legal entities - 5,000+ active users
- **Legal Professionals:** Lawyers, Art.55 structures, mediators - 600+ active professionals
- **Third Parties Mentioned:** Companies involved, witnesses - ~750 companies/year

1.4 Data Recipients

Zorrooo Personnel: Authorized personnel with restricted access according to least privilege principle. Strong authentication mandatory.

Subcontractors (Art. 28 GDPR):

- **Hosting:** OVH France (Roubaix + Gravelines) - ISO 27001, HDS certified, DPA Art. 28 signed, no transfer outside EU

• **Payment:** Stripe (ACPR approved) - PCI-DSS level 1, EU-US transfer: EU Commission standard contractual clauses

• **Other providers:** Analytics (Plausible - Germany), Email (Brevo - France) - All DPA Art. 28 signed, EU hosting

External Recipients:

• **Legal professionals:** Access to dispute data only if citizen initiates private contact

• **Competent authorities:** Upon judicial requisition or legal obligation only

• **No commercial sharing:** No data resale, no advertising profiling

1.5 Retention Periods

Category	Active Period	Intermediate Archive	Justification
User Account	During registration	3 years after closure	Litigation management
Dispute Data	Processing + 6 months	3 years	Civil limitation period
Payments	-	10 years	Accounting obligations
Connection Logs	12 months	-	LCEN obligation
Cookies	13 months max	-	CNIL recommendation
Anonymized Data	Unlimited	-	Outside GDPR scope

1.6 Transfers Outside EU

Principle: No systematic transfer outside EU.

Regulated exception: Stripe (payment processing) - United States

- Guarantee: EU Commission standard contractual clauses (2021)
- Measures: Sensitive data encryption, Transfer Impact Assessment (TIA)

Transparency: Complete subcontractor list available upon request.

PART 2: NECESSITY AND PROPORTIONALITY ASSESSMENT

2.1 Necessity of Processing

Legitimate purposes:

- Access to justice (constitutional objective)
- Alternative dispute resolution (Directive 2013/11/EU, Regulation EU 524/2013)
- Court decongestion (Justice Programming Law)

Solution adopted: Centralized infrastructure with data minimization, public/private space separation, enhanced user control.

2.2 Proportionality of Data Collected

Applied minimization - Data NOT collected:

- ID card/Passport (except professional verification)
- Banking details (managed by Stripe only)
- Browsing history outside platform
- Precise geolocation

Optional data: Profile photo, phone, complete address

2.3 Information to Data Subjects

Enhanced transparency:

- Privacy policy accessible (clear language, short + complete version)
- Contextual information when submitting dispute and contacting professional
- CNIL-compliant cookie banner
- Dedicated 'Your GDPR Rights' page

2.4 Data Subject Rights

Right	Modality
Access (Art. 15)	Automated export (JSON + PDF)
Rectification (Art. 16)	Direct modification in settings
Erasure (Art. 17)	Deletion < 48h
Restriction (Art. 18)	Processing freeze available
Portability (Art. 20)	Structured format (JSON)
Objection (Art. 21)	Dedicated form
Consent (Art. 7)	Withdrawal as simple as giving

Response time: < 1 month (GDPR)

PART 3: RISKS TO RIGHTS AND FREEDOMS

3.1 Assessment Methodology

Severity scale: Negligible | Limited | Significant | Maximum

Likelihood scale: Negligible | Limited | Significant | Maximum

Risk level: Severity × Likelihood

3.2 Risk 1: Unauthorized Access to Dispute Data

Description: Illegitimate access to citizen files (hacking, insider threat).

Impact: Severity MAXIMUM - Privacy violation, moral harm, blackmail, reputation damage

Likelihood: LIMITED (measures in place)

Residual risk: ACCEPTABLE

Technical measures: TLS 1.3 encryption (transit) + AES-256 (at rest), MFA authentication, RBAC authorization, separate databases, network isolation, audited access logs, annual pentests, weekly vulnerability scans

Organizational measures: Staff training, disciplinary sanctions, documented security policy, incident procedure, subcontractor audits

Infrastructure: OVH datacenters (biometric access, 24/7 surveillance, geographic redundancy)

3.3 Risk 2: Non-Consensual Disclosure of Sensitive Data (Art. 9)

Description: Involuntary publication of sensitive data (health, origins, opinions) in dispute descriptions.

Impact: Severity MAXIMUM - Discrimination, stigmatization, dignity harm

Likelihood: SIGNIFICANT (frequent voluntary disclosure)

Residual risk: ACCEPTABLE

Preventive measures: Explicit warning when submitting dispute (red banner), automatic sensitive pattern detection (AI) with user alert, mandatory pseudonym on public forum, supporting documents never public, enhanced erasure right

Corrective measures: Visible 'Report' button, priority processing < 24h, 7/7 moderation team

3.4 Risk 3: Misuse by Professionals

Description: Unauthorized solicitation, list resale, abusive commercial prospecting.

Impact: Severity SIGNIFICANT - Spam, loss of trust, reputation damage

Likelihood: LIMITED

Residual risk: LOW

Contractual measures: Explicit prohibition in TOS (€10,000 penalty clause), mandatory ethics charter

Technical measures: Data access only if citizen initiates contact, suspicious behavior monitoring, invisible watermarking (leak traceability), 3-year history retention

Organizational measures: Manual qualification verification, dedicated reporting procedure, authority transmission if serious violation

3.5 Risk 4: Re-identification of Anonymized Data

Description: Identity reconstruction via cross-referencing of anonymized data.

Impact: Severity SIGNIFICANT - Privacy violation, non-consented profiling

Likelihood: LIMITED

Residual risk: LOW

Technical measures: Robust anonymization (CNIL G29 compliance), minimum k-anonymity k=5, data generalization, unique combination removal, annual external re-identification test, environment separation (prohibited database re-joining)

Organizational measures: Data scientists: anonymized access only, DPO review before statistics publication, prohibition of publication < 10 individuals

3.6 Risk 5: Accidental Data Loss/Destruction

Description: Definitive loss following technical incident (crash, human error, disaster).

Impact: Severity SIGNIFICANT - Loss of evidence, inability to continue processing

Likelihood: LIMITED (redundant infrastructure)

Residual risk: LOW

Technical measures: Automated backups (daily 7d, weekly 4w, monthly 3m), infrastructure redundancy (RAID 10, synchronous replication, multi-AZ), real-time monitoring, 24/7 on-call, documented DRP: RPO 24h, RTO 4h

Organizational measures: Team training, annually tested restoration procedures, staging environment, change validation, post-mortem incidents

Contractual measures: OVH SLA 99.9%, cyber-risk insurance

3.7 Risk 6: Non-Compliance of Cross-Border Processing (Stripe)

Description: Data transfer to United States (Stripe) potentially non-compliant.

Impact: Severity SIGNIFICANT - US surveillance, sovereignty violation

Likelihood: LIMITED (compensatory measures)

Residual risk: ACCEPTABLE

Legal measures: EU Commission standard contractual clauses (SCC) 2021, Transfer Impact Assessment (TIA) conducted, annual review

Technical measures: Enhanced end-to-end encryption (AES-256 + RSA-4096), pseudonymization, payment/dispute data dissociation, transferred volume minimization

Organizational measures: Legal monitoring (CJEU), user transparency, EU alternatives evaluation, EU provider roadmap 2027

3.8 Risk Mapping Summary

Risk	Severity	Likelihood	Initial Level	Residual Level	Acceptable
Unauthorized access	Maximum	Limited	HIGH	ACCEPTABLE	✓
Sensitive data Art. 9	Maximum	Significant	CRITICAL	ACCEPTABLE	✓
Professional misuse	Significant	Limited	MODERATE	LOW	✓
Re-identification	Significant	Limited	MODERATE	LOW	✓
Data loss	Significant	Limited	MODERATE	LOW	✓
Stripe transfer	Significant	Limited	MODERATE	ACCEPTABLE	✓

Conclusion: All identified risks are controlled thanks to implemented technical and organizational measures.

PART 4: PLANNED MEASURES

4.1 Technical Measures

Infrastructure security: TLS 1.3 encryption (transit) + AES-256 (at rest), MFA authentication, RBAC controls, logging + monthly audit, annual pentests, weekly scans, WAF + anti-DDoS, automated 3-2-1 backups, multi-AZ redundancy

Data protection: Non-prod environment pseudonymization, robust anonymization (k-anonymity ≥5), automatic sensitive data detection, database separation, end-to-end messaging encryption

User controls: Automated data export, account deletion < 48h, granular consent management, CNIL-compliant cookie banner

4.2 Organizational Measures

Governance: Designated DPO, up-to-date processing register, documented security policy, incident response procedure, quarterly security committee

Training: Mandatory security onboarding, quarterly reminders, annual GDPR training

Contractualization: Art. 28 DPA with all subcontractors, audit before contractualization, annual compliance review

Continuous compliance: GDPR legal monitoring, annual DPIA review, automated compliance tests

4.3 Privacy by Design

Architecture: Minimization by default, public/private space separation, native forum pseudonymization, facilitated deletion

Features: User visibility control, sensitive data alert, consultable action history, machine-readable export

Default settings: Private profile (opt-in visibility), strictly necessary cookies only, no third-party tracking, random pseudonym generated

4.4 Transparency

- Detailed privacy policy
- Cookie policy
- 'Your GDPR Rights' page
- Accessible subcontractor list
- Annual transparency report

PART 5: VALIDATION AND MONITORING

5.1 Validation

- **Technical validation:** CTPO - 15/01/2026
- **Legal validation:** External counsel - 18/01/2026
- **DPO validation:** 20/01/2026
- **Management validation:** CEO - 22/01/2026

5.2 CNIL Consultation

Art. 36 GDPR Assessment: CNIL consultation mandatory if high risk despite measures.

Conclusion: No CNIL consultation necessary. All residual risks acceptable or low.

5.3 Monitoring Plan

Mandatory annual review: January each year

Exceptional review if:

- New purpose/data category
- New critical subcontractor
- Transfer to new third country
- Major security incident
- Impactful CNIL/CJEU decision

Monitoring indicators:

- Infrastructure availability >99.9%
- Rights response time <15d
- GDPR incidents: target 0
- Sensitive data detection rate >90%

5.4 Responsibilities

- **DPO:** DPIA management, compliance advice, CNIL contact point
- **CTPO:** Technical measures implementation, security architecture
- **CEO:** Strategic validation, resource allocation, final responsibility
- **Support:** Rights requests processing, reporting management

5.5 Associated Documentation

- Processing register (Art. 30 GDPR)
- IS security policy

- Data breach management procedure
- Subcontractor DPAs
- Stripe TIA
- Cookie policy
- TOS/Privacy policy

CONCLUSION

Overall Summary

Zorrooo has implemented a rigorous data protection approach:

- **Privacy by Design:** Architecture minimizing collection and maximizing user control
- **Enhanced security:** Encryption, France hosting, regular audits
- **Transparency:** Clear policy, facilitated rights, annual report
- **Compliance:** Art. 28 contracts, documented TIA, up-to-date register

Overall Risk Level

All identified risks are controlled:

- Unauthorized access: ACCEPTABLE
- Sensitive data Art. 9: ACCEPTABLE
- Professional misuse: LOW
- Re-identification: LOW
- Data loss: LOW
- Stripe transfer: ACCEPTABLE

CNIL Consultation

Not necessary (Art. 36 GDPR): Implemented measures bring all risks to an acceptable level.

Continuous Improvement Commitment

Zorrooo commits to:

- Systematic annual DPIA review
- Reactive update if processing evolution
- Continuous security investment
- Proactive regulatory monitoring

Document approved by:

- CEO Zorrooo SAS
- CTPO Zorrooo SAS
- DPO Zorrooo
- External legal counsel

Approval date: January 22, 2026

Next review: January 2027

Version: 1.0

Contact: support@zorr.ooo

Website: https://zorrooo.com

GDPR documentation: https://zorrooo.com/confidentialite