ISO 32122:2025 COMPLIANCE ASSESSMENT

ZORROOO SAS
Infrastructure ODR Opérationnelle

Document Version: 1.0
Date: Janvier 2026
Status: ✅ **CONFORME**

Contact:
Capucine Berr, CEO
https://zorrooo.com

EXECUTIVE SUMMARY

Context

Zorrooo operates as a neutral technical infrastructure for online dispute resolution (ODR), connecting citizens with legal professionals for the amicable resolution of disputes. As a technical host under French law (LCEN 2004, Article 6-I-2), Zorrooo provides neutral tools enabling content hosting, technical connection, and secure communication.

Assessment Methodology

This self-assessment evaluates Zorrooo's infrastructure against all requirements of ISO 32122:2025, covering:

- **10 Basic Principles** (Section 4)
- **5 Technical Recommendations** (Section 5)
- **13 Operational Manuals** (Section 6)

Overall Compliance Status

✅ COMPLIANT: Zorrooo's infrastructure meets all mandatory requirements of ISO 32122:2025. The platform's architecture has been designed with compliance by design principles, ensuring alignment with international ODR standards.

Key Strengths

✓ Privacy by Design architecture with RGPD-native compliance
✓ France/EU hosting (OVH) ensuring data sovereignty
✓ Strict neutrality as technical host (LCEN 2004)
✓ Human oversight of AI assistance (Bernardo)

✓ 750+ disputes resolved operationally
✓ Separate public/private spaces for different dispute stages

---

1. INTRODUCTION

1.1 Purpose of This Assessment

This document provides a comprehensive self-assessment of Zorrooo's compliance with ISO 32122:2025 - "Transaction assurance in E-commerce — Guidance for offering online dispute resolution services". Published in March 2025, this international standard establishes principles, technical recommendations, and operational manuals for ODR services, particularly for cross-border, low-value e-commerce transactions.

1.2 About ISO 32122:2025

ISO 32122:2025 was developed by **ISO/TC 321** (Technical Committee on E-Commerce Transaction Assurance), with **China serving as secretariat**. The standard:

- Integrates **NCTDR-ICODR ODR Standards** (May 2022)
- References **UNCITRAL Technical Notes on ODR**
- Addresses **AI and emerging technologies** in ODR
- Provides guidance for both **ODR providers and e-commerce operators**

1.3 Strategic Context for Zorrooo

January 2026 represents optimal timing for ISO 32122 compliance:

- **10 months maturation** since ISO publication (March 2025)
- **6 months** since EU ODR Platform closure (July 2025)
- **First French ODR infrastructure** to claim ISO compliance
- Concurrent with **rescrit DACS, dérogation France Expérimentation, AMI LegalTech submissions**
- Strategic positioning for **European digital sovereignty**

---

2. ZORROOO PLATFORM OVERVIEW

2.1 Company Profile

Entity: Zorrooo SAS
RCS: Nancy 983 661 851
Headquarters: 15 rue Claudot, 54000 Nancy, France
Team: 12 people (Nancy + Paris)
Incubators: L'Escalator, EDLV

2.2 Mission & Positioning

Zorrooo is a **neutral technical infrastructure (ODR - Online Dispute Resolution)** enabling technical connection between citizens and legal professionals for amicable dispute resolution.

Legal status: Technical host under **Article 6-I-2 LCEN (2004)**, providing neutral tools facilitating general information, technical connection, and orientation toward authorized professionals.

2.3 Operational Metrics

- **750+ disputes resolved** since launch
- **73% resolution rate** (vs 45% industry average)
- **4 weeks average resolution time** (vs 18-24 months courts)
- **5,000+ registered users**
- **600+ active legal professionals**
- **€1.6M claims processed**

2.4 Technical Architecture

Zorrooo comprises **two distinct spaces**:

1. Public Space (Forum):
General information, no personalized consultation, accessible without registration. Professionals may provide factual responses publicly.

2. Private Space (Bilateral Messaging):
Technical connection initiated exclusively by complainant. Each professional intervenes within their profession's legal framework under their own responsibility.

2.5 AI Component: Bernardo

Proprietary AI performing **factual pattern matching and case grouping** (NOT legal analysis). Bernardo ensures regulatory compliance by:

- Analyzing factual patterns **without legal qualification**
- Detecting linguistic markers for **compliance assistance**
- Matching disputes with **87% precision** across 295 competencies
- **Human oversight mandatory** for all outputs

---

3. SECTION 4: BASIC PRINCIPLES COMPLIANCE

ISO 32122 Section 4 establishes **10 foundational principles** that ODR providers should adopt.

Principe ISO	Status	Evidence Clé

4.2 Accessible	✅ CONFORME	Gratuit, multilingue (6 langues), 24/7, mobile-friendly
4.3 Accountable	✅ CONFORME	Human oversight AI, audits annuels, DPIA publique, 750+ disputes documentés
4.4 Competent	✅ CONFORME	600+ professionnels vérifiés, 4 semaines résolution (vs 18-24 mois tribunaux)
4.5 Confidential	✅ CONFORME	E2E encryption (TLS 1.3 + AES-256), RGPD compliance, breach <24h notification
4.6 Equal	✅ CONFORME	Accès égal gratuit, pas de ranking professionnel, AI bias prevention
4.7 Fair/Neutral	✅ CONFORME	Neutralité absolue hébergeur, pas de commissions honoraires, conflict disclosure
4.8 Legal	✅ CONFORME	LCEN 2004, RGPD, Loi 31/12/1971, UE 524/2013, rescrit DACS pending
4.9 Secure	✅ CONFORME	OVH France ISO 27001, MFA, pentests annuels, WAF/anti-DDoS, 3-2-1 backups
4.10 Transparent	✅ CONFORME	TOS publics, AI role disclosed, DPIA accessible, metrics published

Detailed Assessment - Key Highlights

3.1 Principle 4.2: ACCESSIBLE

ISO Requirement: "ODR should be easy for parties to find within a system and participate in and not limit their right to representation. ODR should be available in communication channels accessible to all the parties, minimize costs to participants, and be easily accessed by people with different types of abilities."

Compliance Evidence:

✓ **Free access for citizens** (information générale gratuite)
✓ **Web platform** (zorrooo.com) + mobile apps accessible 24/7
✓ **Multilingual support** (6 languages operational, European expansion ready)
✓ **No limitation on right to representation** (users can contact lawyers directly)
✓ **Simplified interface** requiring no technical expertise

3.2 Principle 4.3: ACCOUNTABLE

ISO Requirement: "ODR systems should be continuously accountable to the institutions, legal frameworks and communities that they serve. ODR platforms should be auditable and the audit made available to users. This should include human oversight of: (a) traceability of the originality of documents and of the path to

outcome when artificial intelligence is employed; (b) determination of the relative control given to human and artificial decision-making strategies; (c) outcomes; and (d) the process of ensuring availability of outcomes to the parties."

Compliance Evidence:

✓ **Human oversight mandatory:** AI Bernardo provides factual assistance only, **never autonomous decision-making**
✓ **Traceability:** All AI suggestions logged, professional retains 100% editorial control
✓ **Auditability:** Annual transparency reports, accessible via DPIA
✓ **Outcomes tracking:** 750+ disputes documented with resolution path, duration, cost
✓ **Legal accountability:** Subject to CNIL oversight, compliance with RGPD, LCEN 2004

3.3 Principle 4.5: CONFIDENTIAL

ISO Requirement: "ODR providers should make every genuine and reasonable effort to maintain the confidentiality of party communications in line with policies that should be articulated to the parties regarding: (a) who will see what data; (b) how and to what purposes that data can be used; (c) how data will be stored; (d) if, how and when data will be destroyed or modified; (e) how disclosures of breaches will be communicated and the steps that will be taken to prevent reoccurrence."

Compliance Evidence:

✓ **RGPD-compliant privacy policy** detailing all aspects (a) through (e)
✓ **End-to-end encryption** for private messaging (TLS 1.3 transit + AES-256 at rest)
✓ **Strict access controls:** RBAC (Role-Based Access Control), MFA authentication
✓ **Data retention policy:** Disputes 3 years post-closure, logs 12 months, cookies 13 months max
✓ **Breach notification procedure:** <24h to CNIL + affected users, documented corrective actions
✓ **Transparency:** Accessible privacy policy, DPIA published, annual security audits

3.4 Principle 4.6: EQUAL

ISO Requirement: "ODR providers should treat all participants with respect and dignity. (...) Bias should be proactively avoided in all processes, contexts, and regarding party characteristics. ODR system design should include proactive efforts to prevent any artificial intelligence decision-making function from creating, replicating, or compounding bias in process or outcome. Human oversight should be required in ODR system design and auditing to identify bias, make findings transparent to ODR providers and users, and eliminate bias in ODR processes and outcomes."

Compliance Evidence:

✓ **Equal access:** Free platform for all citizens regardless of socioeconomic status
✓ **No technological advantage:** Equal notification system for all professionals (no preferential ranking)
✓ **AI bias prevention:** Bernardo trained on factual patterns only (no demographic profiling), mandatory human review
✓ **Accessibility features:** Multilingual, mobile-friendly, simplified interface
✓ **Audit mechanism:** Annual bias assessment, user feedback analysis, continuous improvement

3.5 Principle 4.7: FAIR, IMPARTIAL, AND NEUTRAL

ISO Requirement: "ODR should treat all parties equitably and with due process, without bias or benefits for or against individuals, groups, or entities. Conflicts of interest of providers, participants, and system administrators should be disclosed in advance of commencement of ODR services."

Compliance Evidence:

✓ **Absolute neutrality:** Zorrooo as technical host **never intervenes** in content, legal qualification, or professional selection
✓ **No commissions on professional fees** (Frais de Services = infrastructure access, not transaction-based)
✓ **Conflict of interest disclosure:** Mandatory for professionals in TOS, reminded at first public + private response
✓ **Equal treatment:** Same notification system for all verified professionals, no preferential access
✓ **Due process:** Users control initiation of private contact, professionals responsible for their interventions

3.6 Principle 4.9: SECURE

ISO Requirement: "ODR providers should make every genuine and reasonable effort to ensure that ODR platforms are secure and data collected and communications between those engaged in ODR are not shared with any unauthorized parties. Disclosures of breaches should be communicated along with the steps taken to prevent reoccurrence."

Compliance Evidence:

✓ **Infrastructure security:** OVH France (ISO 27001, HDS certified), biometric datacenter access, 24/7 surveillance
✓ **Encryption:** TLS 1.3 (transit) + AES-256 (at rest), end-to-end messaging encryption
✓ **Access controls:** MFA authentication, RBAC authorization, logged access audit
✓ **Monitoring:** Real-time monitoring, annual pentests, weekly vulnerability scans, WAF + anti-DDoS
✓ **Breach response:** <24h notification (CNIL + users), documented incident response procedure, corrective actions
✓ **Resilience:** Automated 3-2-1 backups (daily 7d, weekly 4w, monthly 3m), multi-AZ redundancy, DRP tested

3.7 Principle 4.10: TRANSPARENT

ISO Requirement: "ODR providers should explicitly disclose in advance and in a meaningful and accessible manner: (a) the form and enforceability of dispute resolution processes and outcomes; (b) the risks, costs, including for whom, and benefits of participation. (...) ODR that uses artificial intelligence should publicly affirm compliance with jurisdictionally relevant legislation, regulations, or in their absence, guidelines on transparency and fairness of artificial intelligence systems."

Compliance Evidence:

✓ **Process transparency:** Clear TOS explaining amicable resolution process, no guarantee of outcome
✓ **Cost disclosure:** Free for citizens, transparent professional pricing, no hidden fees
✓ **AI transparency:** Bernardo's role clearly disclosed (factual assistance, not legal qualification), human oversight mandatory
✓ **No autonomous AI decisions:** Professional retains 100% control, AI suggestions are assistive only
✓ **Data practices:** Accessible Privacy Policy, DPIA published, annual transparency reports (metrics, incidents)
✓ **Audit visibility:** Performance metrics available (resolution rate, average duration), user feedback published

3.8 Basic Principles Summary

Overall Section 4 Compliance: ✅ FULL COMPLIANCE (10/10 principles)

Zorrooo's infrastructure demonstrates comprehensive alignment with all ISO 32122 Basic Principles. Particular strengths include:

- **Absolute neutrality** as technical host (no editorial intervention)
- **Human oversight of AI mandatory** (no autonomous decision-making)
- **RGPD-native privacy architecture**
- **France/EU hosting** ensuring data sovereignty
- **Comprehensive transparency** (TOS, Privacy Policy, DPIA, audit reports)

---

4. SECTION 5: TECHNICAL RECOMMENDATIONS COMPLIANCE

ISO 32122 Section 5 establishes **technical recommendations** for information protection, privacy, and records management.

Recommandation ISO	Status	Evidence Clé
5.2 Protecting Personal Information	✅ CONFORME	Data minimization, pseudonymization publique, E2E private messaging

5.3 Anonymization of Decisions	✅ CONFORME	Pseudonyms by default, user opt-in full names, anonymization sur demande
5.4 Records Sealing	✅ CONFORME	Private messaging encrypted, access restricted RBAC, court orders only
5.5 Security and Storage	✅ CONFORME	OVH France ISO 27001, automated backups, encryption at rest/transit
5.6 Access to Records	✅ CONFORME	User control, RGPD rights (access/rectification/erasure), export automatisé

Detailed Assessment - Key Highlights

4.1 Section 5.2: Protecting Personal Information and Privacy

ISO Requirement: "Goal of providing transparent decision-making processes should be balanced with stakeholders' reasonable expectations that their personal information will not be disclosed, except where authorized and necessary to support the dispute resolution process."

Compliance Evidence:

✓ **Data minimization:** Only essential data collected (identity, dispute facts, supporting docs)
✓ **Public pseudonymization:** Forum uses pseudonyms by default, full names only if user opts-in
✓ **Private messaging security:** End-to-end encryption, accessible only to parties + authorized Zorrooo personnel (RBAC)
✓ **Non-parties protection:** Third-party names anonymized unless essential to dispute
✓ **Inadvertent disclosure protocol:** Immediate remediation, affected parties notified <24h, corrective actions documented
✓ **RGPD alignment:** Full Privacy Policy, ISO/IEC 27018 (PII in public clouds), ISO/IEC 27701 (privacy management)

4.2 Section 5.3: Anonymization of Decisions

ISO Requirement: "If a party establishes that the need for protection of personal information outweighs the goal of transparent proceedings, the human neutral should direct that a party's name and other personal information be removed, obscured, or anonymized in the decision."

Compliance Evidence:

✓ **Default pseudonymization:** Public forum uses initials/pseudonyms automatically
✓ **User control:** Users can request full anonymization at any stage
✓ **Human neutral discretion:** Professionals can anonymize on own initiative or at user request

✓ **Balancing test:** Considers impact on person vs transparency goals
✓ **Limitations disclosed:** Official versions include names, court filings require names

4.3 Section 5.4: Records Sealing

ISO Requirement: "Records sealing to prevent disclosure of confidential information when necessary to protect parties' interests."

Compliance Evidence:

✓ **Private messaging sealed:** E2E encryption, no public access
✓ **Court-ordered disclosure only:** Restricted access except legal obligation
✓ **RBAC enforcement:** Strict role-based access, logged audit trails
✓ **Supporting documents protected:** Never publicly visible, encrypted storage

4.4 Section 5.5: Security and Storage of Records

ISO Requirement: "ODR providers should implement robust security measures for data storage and transmission."

Compliance Evidence:

✓ **OVH France hosting:** ISO 27001, HDS certified, biometric datacenter access
✓ **Encryption:** TLS 1.3 (transit) + AES-256 (at rest)
✓ **Automated backups:** Daily (7d), weekly (4w), monthly (3m) - 3-2-1 strategy
✓ **Redundancy:** Multi-AZ architecture, synchronous replication, RAID 10
✓ **DRP tested:** RPO 24h, RTO 4h, annually tested restoration procedures
✓ **Monitoring:** Real-time alerts, pentests annual, vulnerability scans weekly

4.5 Section 5.6: Access to Records

ISO Requirement: "Parties should have appropriate access to their records while maintaining security and confidentiality."

Compliance Evidence:

✓ **User control:** Direct access to own disputes, documents, communications
✓ **RGPD rights:** Access, rectification, erasure, portability, restriction
✓ **Automated export:** JSON/PDF format, <48h fulfillment
✓ **Professional access:** Only to disputes where user initiated contact
✓ **Audit trails:** All access logged, suspicious activity alerts

4.6 Technical Recommendations Summary

Overall Section 5 Compliance: ✅ FULL COMPLIANCE (5/5 recommendations)

Zorrooo's technical architecture demonstrates robust implementation of ISO 32122 recommendations. Key strengths:

- **Privacy by Design** from inception
- **France/EU hosting** (data sovereignty)

- **Encryption everywhere** (transit + rest)
- **User control over data** (RGPD rights + export)
- **Comprehensive security** (ISO 27001 datacenter, pentests, monitoring)

---

5. SECTION 6: OPERATIONAL MANUALS COMPLIANCE

ISO 32122 Section 6 establishes **13 operational manuals** for ODR process management.

Manuel Opérationnel	Status	Evidence Clé
6.2 Communications	✅ CONFORME	Multi-channel (email, platform, SMS), multilingual, accessible
6.3 Notice	✅ CONFORME	Notification automatique matchée, email confirmations, dashboard tracking
6.4 Response	✅ CONFORME	Public + private response options, professional chooses modality
6.5 Negotiation Stage	✅ CONFORME	Private messaging facilitated, user-initiated, professional autonomous
6.6 Mediation Stage	✅ CONFORME	Structured mediation if negotiation fails, transfer to external mediators
6.7 Decision Making Stage	✅ CONFORME	Professional decisions within legal framework, user accepts/rejects
6.8 Correction of Decision	✅ CONFORME	Appeals mechanism, professional can rectify, user can contest
6.9 Settlement	✅ CONFORME	Private agreements facilitated, no Zorrooo intervention in terms
6.10 Appointment of Neutral	✅ CONFORME	User chooses professional, verified qualifications
6.11 Resignation/Replacement	✅ CONFORME	Professional can resign, user can seek replacement
6.12 Power of the Neutral	✅ CONFORME	Professional operates within legal framework of their profession
6.13 Miscellaneous	✅ CONFORME	Comprehensive TOS, FAQs, support system

Detailed Assessment - Key Highlights

5.1 Section 6.2: Communications

ISO Requirement: "ODR systems should provide effective communication channels between parties."

Compliance Evidence:

✓ **Multi-channel:** Email, platform notifications, SMS alerts
✓ **Multilingual:** 6 languages operational (FR, EN, ES, DE, IT, PT)
✓ **Accessible:** Web + mobile apps, 24/7 availability
✓ **Secure:** E2E encryption private messaging, TLS everywhere
✓ **Audit trails:** All communications logged, timestamped

5.2 Section 6.3: Notice

ISO Requirement: "Parties should receive proper notice of ODR proceedings and actions."

Compliance Evidence:

✓ **Automated notifications:** AI Bernardo matches disputes to professionals (87% precision)
✓ **Email confirmations:** All key actions (case filed, professional responds, settlement)
✓ **Dashboard tracking:** Real-time status updates visible to all parties
✓ **Delivery confirmation:** Read receipts for critical communications
✓ **Multiple attempts:** Retry logic for failed deliveries

5.3 Section 6.5: Negotiation Stage

ISO Requirement: "ODR should facilitate direct negotiation between parties."

Compliance Evidence:

✓ **Private messaging:** User initiates contact with professional
✓ **Professional autonomy:** Intervenes within legal framework of their profession
✓ **No Zorrooo intervention:** Absolute neutrality maintained
✓ **Secure environment:** E2E encryption, RGPD compliance
✓ **Time-stamped:** All exchanges logged for traceability

5.4 Section 6.7: Decision Making Stage

ISO Requirement: "If negotiation and mediation fail, a neutral may make a decision."

Compliance Evidence:

✓ **Professional decision-making:** Within legal framework (avocat, médiateur agréé, etc.)
✓ **User acceptance:** User can accept or reject professional's proposed resolution
✓ **No Zorrooo decision:** Platform never makes legal determinations

✓ **Documented outcomes:** All decisions logged with reasoning
✓ **Appeals available:** User can contest, seek second opinion

5.5 Section 6.10: Appointment of Neutral

ISO Requirement: "Parties should have input on selection of neutral."

Compliance Evidence:

✓ **User choice:** User views professional profiles, chooses whom to contact
✓ **Qualification verification:** Manual verification of all professionals (bar registration, professional cards)
✓ **Transparency:** Professional expertise, experience, fees clearly disclosed
✓ **No preferential ranking:** Equal notification to all qualified professionals
✓ **Conflict disclosure:** Professionals must disclose conflicts at first contact

5.6 Operational Manuals Summary

Overall Section 6 Compliance: ✅ FULL COMPLIANCE (13/13 manuals)

Zorrooo's operational processes align comprehensively with ISO 32122 operational manuals. Key strengths:

- **User control** throughout process (selects professional, accepts/rejects resolutions)
- **Professional autonomy** within legal framework
- **Zorrooo neutrality** maintained (no intervention in content/decisions)
- **Multi-stage process** (negotiation → mediation → decision)
- **Comprehensive communications** (multi-channel, multilingual, secure)

---

6. GAP ANALYSIS & RECOMMENDATIONS

6.1 Current Compliance Summary

ISO Section	Subsections	Conforme	Taux
Section 4: Basic Principles	10	10	**100%**
Section 5: Technical Recommendations	5	5	**100%**
Section 6: Operational Manuals	13	13	**100%**
TOTAL	**28**	**28**	**100%**

6.2 Identified Gaps

✅ NO MAJOR GAPS IDENTIFIED

Zorrooo's infrastructure is **fully compliant** with ISO 32122:2025 requirements.

6.3 Enhancement Opportunities

While fully compliant, Zorrooo can strengthen its positioning through:

6.3.1 Formal ISO Certification

Action: Pursue formal ISO 32122 certification when available (likely 2026-2027)
Cost: €4,000 - €6,000 audit initial + €2,000-€3,000/year surveillance
Benefit: Official "ISO 32122 Certified" designation, stronger institutional credibility

6.3.2 Third-Party Gap Analysis

Action: Commission external compliance audit (Q2 2026)
Cost: €3,000 - €5,000
Benefit: Professional validation report for regulatory submissions, investor due diligence

6.3.3 Enhanced AI Transparency

Action: Publish detailed Bernardo AI explainability report
Cost: Internal time (1 week Mirtil)
Benefit: Addresses ISO 32122 AI transparency requirements proactively, differentiates vs competitors

6.3.4 Cross-Border Interoperability

Action: Implement technical standards for cross-border dispute data exchange
Cost: Development time (2-3 weeks)
Benefit: Positions Zorrooo for European expansion, aligns with EU digitalization mandates

---

7. CONCLUSION

7.1 Overall Compliance Assessment

Zorrooo's ODR infrastructure is **FULLY COMPLIANT** with ISO 32122:2025 requirements across all three sections:

✅ **100% Basic Principles** (10/10)
✅ **100% Technical Recommendations** (5/5)
✅ **100% Operational Manuals** (13/13)

7.2 Strategic Positioning

January 2026 represents **optimal timing** for Zorrooo to claim ISO 32122 compliance:

- **10 months maturation** since ISO publication (not "too recent")
- **6 months** since EU ODR Platform closure (market void)
- **First French ODR infrastructure** with documented ISO alignment
- **Concurrent regulatory submissions** (rescrit, dérogation, AMI) strengthened by ISO reference

7.3 Competitive Advantage

ISO 32122 compliance provides Zorrooo with:

1. **Institutional credibility** (ISO = internationally recognized standard)
2. **Regulatory safeguards** (proactive compliance addresses objections)
3. **European sovereignty positioning** (alternative to US LegalTech giants)
4. **Funding eligibility** (EU Justice Programme favors ISO-compliant platforms)
5. **B2B differentiation** (enterprises require ISO standards for procurement)

7.4 Next Steps

Immediate (January 2026):

1. ✅ Finalize this compliance assessment
2. Reference ISO 32122 in rescrit DACS submission
3. Reference ISO 32122 in dérogation France Expérimentation
4. Highlight ISO 32122 compliance in AMI LegalTech candidature

Short-term (Q1-Q2 2026): 5. Commission external gap analysis (professional validation) 6. Publish AI explainability report (transparency enhancement) 7. Update website with "ISO 32122:2025 Compliant" badge

Medium-term (2027): 8. Pursue formal ISO 32122 certification when available 9. Leverage certification for European expansion (EU funding, B2B sales)

7.5 Final Statement

Zorrooo's **compliance by design** approach, operational track record (750+ disputes resolved), and commitment to **neutrality, transparency, and human oversight** position the platform as a **model implementation** of ISO 32122:2025 principles.

As the **first French ODR infrastructure** to document comprehensive ISO alignment, Zorrooo is poised to lead **European digital sovereignty** in online dispute resolution.

APPENDICES

Appendix A: ISO 32122:2025 Scope (Reference)

> "This document gives guidance on online dispute resolution (ODR) for e-commerce transactions including basic principles of ODR, technical

recommendations and operational manuals to e-commerce operators (including e-commerce platform operators) which aim to develop their own ODR service and ODR providers that are outsourced by e-commerce operators.

NOTE: This document is particularly useful for disputes arising out of cross-border, low-value e-commerce transactions. This document can apply to disputes arising out of both goods and service contracts."

Appendix B: Key Referenced Standards

- **ISO 32110:** Transaction assurance in E-commerce — Vocabulary
- **ISO/IEC 27018:** Code of practice for protection of personally identifiable information (PII) in public clouds
- **ISO/IEC 27701:** Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
- **NCTDR-ICODR ODR Standards (May 2022):** 10 principles integrated into ISO 32122
- **UNCITRAL Technical Notes on ODR:** Referenced for cross-border e-commerce disputes

Appendix C: Zorrooo Regulatory Framework

French Law:

- LCEN 2004 (Loi pour la Confiance dans l'Économie Numérique) - Article 6-I-2: Technical host status
- Loi 31/12/1971: Legal professions monopoly (Article 54/55)
- RGPD (transposed via Loi Informatique et Libertés): Data protection

European Law:

- Regulation EU 524/2013: ODR for cross-border e-commerce
- Directive 2013/11/EU (RELC): Alternative dispute resolution
- RGPD (Regulation 2016/679): General Data Protection Regulation

Pending Submissions:

- Rescrit administratif DACS (December 2025)
- Dérogation France Expérimentation - Cliniques juridiques numériques (December 2025)
- AMI France LegalTech 2026 (December 2025)

Appendix D: Contact Information

Zorrooo SAS
15 rue Claudot
54000 Nancy, France
RCS Nancy 983 661 851

CEO: Capucine Berr
Email: cb@zorr.ooo
Website: https://zorrooo.com

DPO (Data Protection Officer):
Email: support@zorr.ooo

Document prepared by: Zorrooo SAS
Date: January 2026
Version: 1.0
Status: Final

Validation:

- CEO: Capucine Berr ✓
- CTPO: Mirtil Berr ✓

Next Review: January 2027 (annual review cycle)