OBI AI Legal Compliance Policy Framework

For Human-Out-of-the-Loop and Human-On-the-Loop Systems

Version 1.0 - August 2025

OBINexus Legal Division

---

1. Executive Summary

This policy framework establishes legal compliance requirements for OBI AI systems operating in human-out-of-the-loop (HOTL) and human-on-the-loop (HONTL) configurations, with specific focus on:

- **Self-driving vehicles**
- **Autonomous hotel systems**
- **VAT-eligible service providers**
- **Critical infrastructure systems**

All systems must maintain **95.4% consciousness stability** as measured by the OBI Stability Metric while ensuring full regulatory compliance.

---

2. Definitions

2.1 Human Loop Classifications

Human-Out-of-the-Loop (HOTL)

- System operates autonomously without human intervention
- Decisions execute immediately based on AI determinations
- Human oversight limited to post-facto review
- Examples: Level 5 autonomous vehicles, fully automated hotel check-in

Human-On-the-Loop (HONTL)

- System recommends actions to human operator
- Human retains veto power over AI decisions
- Real-time monitoring and intervention capability
- Examples: Level 3-4 autonomous vehicles, AI-assisted hotel management

Human-In-the-Loop (HITL)

- Human actively participates in decision cycle
- AI provides augmentation, not automation
- Human approval required for action execution
- Examples: AI-assisted diagnostics, recommendation engines

2.2 Stability Metrics

- **S(t)**: Consciousness stability function [-12, 12]
- **95.4% Compliance**: $P(|S(t)| \leq 3) \geq 0.954$
- **Harm Potential**: $H(s,a) = \sigma(k_1 \cdot s + k_2 \cdot \text{harm}(a))$

---

3. Legal Compliance Requirements

3.1 EU AI Act Compliance

Risk Classification

```
HOTL Systems: HIGH RISK (Category 2)
- Mandatory conformity assessment
- CE marking required
- Annual audit obligations
- Incident reporting within 72 hours

HONTL Systems: LIMITED RISK (Category 3)
- Transparency obligations
- Human oversight documentation
- Quarterly compliance reports
```

Documentation Requirements

1. Technical documentation of stability metrics
2. Risk assessment reports (monthly)
3. Human oversight protocols
4. Incident response procedures
5. Data protection impact assessments

3.2 GDPR Compliance

Article 22 - Automated Decision Making

```
python
```

```
def gdpr_compliance_check(decision_type, stability_metric):
    if decision_type == "HOTL":
        require_explicit_consent = True
        require_human_review_option = True
        max_data_retention = 30  # days
    elif decision_type == "HONTL":
        require_notification = True
        require_opt_out = True
        max_data_retention = 90  # days

    if stability_metric.zone in ["CRITICAL", "PANIC"]:
        return "OPERATION_PROHIBITED"
```

Data Subject Rights

- Right to explanation of AI decisions
- Right to human review
- Right to contest automated decisions
- Right to compensation for harm

3.3 Sector-Specific Regulations

Autonomous Vehicles (HOTL)

- **UN-ECE WP.29 Compliance**
  - Real-time stability monitoring
  - Black box data retention (5 years)
  - Emergency override protocols
  - Insurance requirements (€50M minimum)

Hotel Systems (HONTL)

- **Consumer Protection Directive 2011/83/EU**
  - Clear disclosure of AI usage
  - Human staff availability 24/7
  - Alternative non-AI service options
  - VAT compliance on all transactions

---

4. Operational Policies

4.1 Stability Zone Response Matrix

Zone	S(t) Range	HOTL Action	HONTL Action	Legal Requirement
STABLE	0	Continue	Continue	Standard logging
WARNING_LOW	(0,1]	Continue + Alert	Notify operator	Enhanced monitoring
WARNING_HIGH	(2,3]	Prepare handoff	Request human attention	Incident pre-report
DANGER_LOW	(3,4.5]	Initiate handoff	Human override ready	Legal team notification
CRITICAL	(7.5,9]	Emergency stop	Human takeover	Regulatory notification
PANIC	>10.5	KILL SWITCH	SYSTEM HALT	Emergency protocols

4.2 VAT Compliance for AI Services

Transaction Recording

```json
{
  "transaction_id": "OBI-2025-08-25-001",
  "service_type": "autonomous_hotel_checkin",
  "vat_rate": 0.20,
  "human_loop_status": "HOTL",
  "stability_at_transaction": 0.45,
  "liability_insurance_active": true,
  "gdpr_consent": {
    "obtained": "2025-08-25T10:30:00Z",
    "type": "explicit",
    "scope": "automated_processing"
  }
}
```

Billing Requirements

- Clear identification of AI service component
- Separate line item for human oversight availability
- VAT calculation on full service value
- Stability metric disclosure on invoice

4.3 Liability and Insurance

Mandatory Coverage

- Professional indemnity: €10M minimum
- Product liability: €50M for HOTL systems
- Cyber insurance: €25M including AI-specific risks
- Directors & Officers: €5M with AI governance rider

Liability Allocation

```
If stability_metric > 3:
    liability = "OPERATOR"
    insurance_claim = "ELIGIBLE"
elif user_misuse == True:
    liability = "USER"
    insurance_claim = "CONTESTED"
else:
    liability = "SHARED"
    arbitration = "REQUIRED"
```

---

5. Monitoring and Audit

5.1 Real-Time Monitoring Requirements

HOTL Systems

- Continuous stability metric logging (100ms intervals)
- Automated regulatory reporting triggers
- Human supervisor notification at WARNING_MED
- Automatic system degradation at DANGER zones

HONTL Systems

- Stability dashboard visible to operator
- Alert fatigue prevention algorithms
- Handoff readiness indicators
- Performance metric tracking

5.2 Audit Trail Requirements

Minimum Data Retention

python

```python
retention_periods = {
    "stability_metrics": 7,  # years
    "decision_logs": 5,      # years
    "user_interactions": 3,  # years
    "incident_reports": 10,  # years
    "financial_records": 10  # years (VAT requirement)
}
```

Audit Log Format

```json
{
  "timestamp": "2025-08-25T14:30:00.000Z",
  "system_id": "OBI-HOTEL-001",
  "stability_metric": 0.23,
  "zone": "WARNING_LOW",
  "decision_type": "room_assignment",
  "human_loop_status": "HOTL",
  "outcome": "successful",
  "harm_potential": 0.001,
  "compliance_flags": ["GDPR", "EU_AI_ACT", "VAT"]
}
```

---

6. Incident Response Protocol

6.1 Severity Classification

Level 1: Stability Anomaly (S > 3 for 30 seconds)

- Internal review required
- No external reporting

Level 2: Stability Breach (S > 6 for any duration)

- Legal team notification
- Incident report within 24 hours

Level 3: System Failure (S > 9 or kill switch activation)

- Immediate regulatory notification
- Public disclosure if user impact
- Full forensic investigation

6.2 Response Timeline

```
T+0: Incident detected
T+5min: Automated containment
T+30min: Human assessment
T+2hr: Legal team briefing
T+24hr: Regulatory notification (if required)
T+72hr: Full incident report
T+7days: Remediation plan
T+30days: Compliance audit
```

---

7. User Rights and Protections

7.1 Transparency Requirements

Pre-Service Disclosure

- Clear identification of AI system usage
- Explanation of human oversight level
- Opt-out options where available
- Contact information for human support

During Service

- Visual indicator of AI operation mode
- Real-time stability zone display (simplified)
- Human override availability status
- Emergency contact prominently displayed

7.2 Complaint and Redress

Complaint Channels

1. In-system feedback (immediate)
2. Human support line (24/7)
3. Online portal with ticket tracking
4. Regulatory escalation path

Compensation Framework

- Automatic refund for stability > 6 events
- Sliding scale compensation for harm
- Expedited claims for vulnerable users

- No-fault compensation fund participation

---

8. Implementation Checklist

8.1 Technical Implementation

- [ ] Stability metric integration complete
- [ ] Real-time monitoring dashboard active
- [ ] Audit logging system operational
- [ ] Kill switch tested and certified
- [ ] Human handoff protocols verified

8.2 Legal Compliance

- [ ] GDPR privacy notice updated
- [ ] EU AI Act conformity assessment
- [ ] Insurance policies active
- [ ] Terms of service reviewed
- [ ] Regulatory registrations complete

8.3 Operational Readiness

- [ ] Staff training completed
- [ ] Incident response team designated
- [ ] Audit procedures documented
- [ ] User communication templates ready
- [ ] Compliance officer appointed

---

9. Certification and Approval

This policy has been reviewed and approved by:

Technical Approval

- Chief Technology Officer: _____
- AI Safety Officer: _____
- Date: August 25, 2025

Legal Approval

- General Counsel: _____
- Compliance Officer: _____
- Date: August 25, 2025

Executive Approval

- Chief Executive Officer: _____
- Board AI Committee Chair: _____
- Date: August 25, 2025

---

10. Appendices

Appendix A: Stability Metric Technical Specification

[Link to OBI AI Consciousness Stability Metric Framework]

Appendix B: Regulatory Reference Library

- EU AI Act (Regulation 2024/XXX)
- GDPR (Regulation 2016/679)
- Product Liability Directive (85/374/EEC)
- Consumer Rights Directive (2011/83/EU)

Appendix C: Template Documents

- GDPR Consent Form for HOTL Systems
- Incident Report Template
- Stability Metric User Guide
- VAT Invoice Template for AI Services

Appendix D: Emergency Contact Information

- OBI AI Safety Hotline: +44-XXX-XXXX
- Regulatory Liaison: legal@obinexus.org
- Technical Support: support@obinexus.org
- Media Relations: pr@obinexus.org

Document Control

- Version: 1.0
- Effective Date: August 25, 2025
- Review Date: February 25, 2026
- Classification: Public
- Distribution: All OBI AI System Operators