Ethical Risk Assessment

Stakeholders & Context

Understanding who is affected and why ethical alignment matters

Business Context

- **Company:** VPS Hosting is a compact, engineer-led organization where several responsibilities overlap.
- **Project goal:** Use data science to identify recurring issues and improve internal efficiency and customer experience.
- **Data used:** Chat and email support logs (≈ 5000 + 150 threads), 2021 – 2025.
- **Scope:** Internal analytics only — no automated decisions or profiling.

Ethical anchor: Responsible use of customer communication data to enhance service quality while preserving privacy and trust.

Ethical Relevance

- Each stakeholder has different risk exposure, from privacy to fairness and reliability.
- The assessment aligns ethical responsibilities with organizational roles to ensure shared accountability.
- Ethical design is treated as a trust and retention strategy.

Role / Stakeholder	Responsibility	Ethical Relevance
Customers	Provides communication data via support	Privacy, fairness, transparency
Support Engineers	Responds to users, validates clusters, updates FAQ	Accuracy, human oversight
Security Engineers	Manage infrastructure and access controls	Data breach risk, audit trail integrity
Data Analyst	Builds models, manages data, ensures anonymization	Data governance, bias mitigation
Product & Security responsibility	Oversees operational goals and secure infrastructure	Balance efficiency with safety
Legal / DPO	Reviews GDPR/AI Act compliance	Lawful basis, minimization, data rights
Founder	Approves ethical framework and ensures accountability	Integrity, trust, alignment with company values

Data Flow & Purpose Limitation

How customer data is handled responsibly within the analytics workflow

Data Flow Overview

1. Collection

Customer interactions from support channels are exported from the ticketing system.

Contain timestamps, message text, sender type, metadata.

2. Cleaning & Anonymization

Personal identifiers (emails, IPs, names) are masked before analysis.

This step enforces *data minimization* and *privacy by design*.

3. Feature Extraction

Only analytical attributes are derived (TF-IDF terms, sentiment, message length, named entities).

No profiling or user tracking.

4. Clustering & Validation

Unsupervised model groups tickets by theme. Clusters reviewed manually by Support Lead.

Human oversight ensures interpretability and guards against automation bias.

5. Insight Integration

Findings inform FAQ updates and process optimization.

No automated actions: decisions remain human-driven.

Principle	Implementation in Hexcore Project
Purpose	Data used exclusively for support improvement and internal efficiency.
Lawful Basis (GDPR, EU AI Act)	Legitimate interest: improving customer service quality.
Data Minimization	Only non-personal, task-relevant fields retained for analysis.
Storage Limitation	Raw logs kept up to 24 months for operations and audits. Anonymized datasets retained longer for trend analysis, as they are no longer personal data
Transparency & Oversight	All analytical outcomes reviewed by Support Lead; no external data sharing.

Regulatory Alignment

Anchoring the project in responsible data governance frameworks

GDPR Alignment focuses on lawful, minimal, secure handling of customer data.

EU AI Act Alignment ensures transparency, oversight, and technical reliability of the analytics process.

GDPR Alignment

GDPR	Application in project
Lawfulness & Purpose	Legitimate interest; goal - improving support; no secondary use.
Minimization	After anonymization, only text features remain.
Storage	Raw logs stored up to 24 months; anonymous datasets can be stored longer for trending.
Security & Accountability	Encryption, limited access, audit log, external DPO upon request.

Company process support communications under **GDPR Art. 6(1)(f) – Legitimate Interests** to improve service quality. User benefit and minimization outweigh residual risks. No secondary uses (marketing/ profiling).

EU AI Act

- *Risk management*: manual cluster validation, quality reports.
- *Data governance*: domain-specific dataset, documented preprocessing, language parity.
- *Human oversight*: no automated actions; decisions are made by the Support Lead.
- *Transparency*: pipeline, field schema, and anonymization logic are described.
- *Accuracy & robustness*: silhouette/topic coherence + coverage threshold ≥80%.
- *Security & logging*: secure environment, artifact versioning.

EU Act *Risk class:* Internal analytics → **Minimal risk**
Complies with high-risk principles by choice

Ethical Risk Matrix

Risk Category	Description	Impacted Stakeholders	Mitigation Strategy	Risk Level
Privacy	Sensitive data (IPs, emails) could be exposed or re-identified during preprocessing.	Customers, Support engineers	Strict anonymization pipeline, limited access, audit logs.	🟡 Medium
Bias / Representativeness	Overrepresentation of one language (EN/RU) may distort topic clustering.	Customers	Separate language-based clustering, review for parity.	🟡 Medium
Transparency & Explainability	Clusters may be hard to interpret for non-technical staff.	Support engineers, Management	Human-readable summaries, visual topic maps, internal documentation.	🟢 Low
Human Oversight Risk	Analyst decisions may influence which clusters are prioritized.	Support engineers, Customers	Manual validation by multiple reviewers, consensus-based labeling.	🟢 Low
Security & Data Governance	Unauthorized access to logs or models.	Company, Customers	Controlled environment, encryption, periodic access audits.	🟡 Medium
Future Automation Consideration	If insights later inform automated routing/AI assisted support, risks of bias /misclassification must be reassessed under a dedicated ethical review.	Management, Data team	Not applicable at current stage, flagged for future ethical assessment.	⚪ N/A

The matrix aligns with EU AI Act principles, focusing on fairness, privacy, and human oversight.

Ethical Practices in Company

Substantiating responsible data practices through integrated oversight

As a compact engineering team, company integrates ethical safeguards directly into its workflow — through code transparency, peer validation, and a shared sense of responsibility rather than formal compliance paperwork.

- **Shared accountability** — every team member handling data signs off on anonymization and understands GDPR basics.
- **Transparency by design** — data transformations, clustering logic, and decisions are documented directly in the analysis repo.
- **Human-in-the-loop** — clustering results are always reviewed by engineers who understand customer context before any process change.
- **Privacy-first mindset** — anonymization scripts are part of preprocessing, not a separate legal stage.
- **Ethics as culture, not process** — focus on trust, data minimalism, and continuous awareness.

Aspect	Practice	Responsible
Data privacy	Mask personal data, limit access	Data analyst
Fairness	Check multilingual balance, no user profiling	Support lead
Transparency	Keep all preprocessing steps documented in repo	Entire team
Oversight	Manual review of model outputs	Engineers & founder

Ethical Reflection: Responsibility as Competitive Advantage

Substantiating how responsible data use strengthens both trust and performance

Data ethics is a part of how company build trust with customers, team and with technology.

Working with real customer communication data demands humility and precision: every insight must serve users and company goals.

By integrating privacy-first design and human oversight into everyday workflows, the team reduces operational friction while strengthening reliability and customer retention.

This alignment between *ethical awareness and business value* ensures that data-driven growth remains both sustainable and human-centered.

Ethical Principle	Business Outcome
Data minimization	Reduced data risk, easier compliance
Transparency	Faster debugging and team learning
Fairness	Balanced service quality across languages
Human oversight	Higher trust in automation outcomes
Privacy by design	Stronger customer loyalty

Responsible innovation is not about limiting progress — it’s about designing it with care.