SlideHub ApS AI Framework

EU AI Act Compliance Policy

Version: 1.3
Effective Date: September 18, 2025
Last Reviewed: February 6, 2026
Document Owner: Anders Thomsen (CEO/CTO)

1. Introduction and Scope

1.1 Purpose

This framework establishes SlideHub ApS's governance structure and operational procedures to ensure full compliance with Regulation (EU) 2024/1689 (the EU AI Act) in the development, deployment, and use of AI systems within our presentation platform.

1.2 Scope

This policy applies to all AI features and functionalities integrated into SlideHub's platform, specifically those powered by Groq and Cloudflare AI Workers, including but not limited to:

- Content generation and suggestions
- Presentation design automation
- Text analysis and optimization
- Image processing and enhancement
- Any future AI-powered features

1.3 Key Principles

- **Non-retention Architecture**: Leveraging providers that do not store input/output tokens
- **No Training on User Data**: Absolute prohibition on training AI models using user inputs, outputs, or stored content
- **Transparency**: Clear communication about AI use to all users
- **Human Oversight**: Maintaining meaningful human control over AI outputs
- **Privacy by Design**: Embedding data protection throughout the AI lifecycle
- **Continuous Compliance**: Regular assessment and updates to maintain compliance

2. Risk Classification and Assessment

2.1 System Classification

Based on EU AI Act Annex III, SlideHub's AI systems are classified as **Limited Risk** systems, as they:

- Generate or manipulate content (presentations)
- Do not fall under high-risk categories
- Do not engage in prohibited practices

2.2 Risk Assessment Framework

2.2.1 Initial Risk Assessment

- **Frequency**: Before deploying any new AI feature
- **Scope**: Evaluate intended use, potential misuse, and impact on users
- **Documentation**: Maintain risk assessment records for 5 years minimum

2.2.2 Ongoing Risk Monitoring

- Quarterly reviews of AI system performance
- User complaint analysis
- Incident tracking and response
- Annual comprehensive risk reassessment

2.3 Risk Mitigation Measures

- Implementation of content filters for harmful or inappropriate content
- User authentication and access controls
- Rate limiting to prevent abuse
- Regular security assessments of AI endpoints

3. Transparency and User Information

3.1 AI Interaction Disclosure

Users must be informed when interacting with AI systems through:

- Clear labelling of AI-generated content
- Visible indicators when AI features are active
- Distinction between AI suggestions and user-created content

3.2 Information Provision Requirements

The following information must be readily accessible to users:

- Nature and purpose of AI features
- Data processing activities (emphasizing no storage by AI providers)
- **Explicit commitment that user data is never used for AI model training**
- Guarantee that SlideHub library content is never used for model improvement
- Human oversight mechanisms
- User rights regarding AI-generated content
- Contact information for AI-related inquiries

3.3 Documentation Requirements

- Maintain updated technical documentation of AI systems
- Keep records of AI model versions and updates
- Document decision logic and training approaches used by providers
- Preserve audit trails of significant AI deployments

4. Data Governance and Privacy

4.1 Data Processing Principles

- **Minimal Data Transfer**: Only send necessary data to AI providers
- **No Persistent Storage**: Verify and monitor that Groq and Cloudflare maintain no-storage policies
- **Strict No-Training Policy**: Absolute prohibition on using user data for model training
- **Purpose Limitation**: Use AI only for declared purposes
- **Data Minimization**: Process only data essential for the requested function

4.2 Prohibition on Model Training

SlideHub ApS commits to the following strict policies:

- **No Training on User Inputs**: User prompts, queries, and inputs will never be used to train, fine-tune, or improve AI models
- **No Training on AI Outputs**: Generated content will never be used for model training purposes
- **No Training on Library Content**: Presentations, templates, and content stored in SlideHub's library will never be used for AI model development
- **No Data Sharing for Training**: User data will never be shared with third parties for model training purposes
- **Contractual Enforcement**: All provider agreements must include clauses prohibiting training on SlideHub user data

4.3 Data Protection Measures

- Encryption of data in transit to AI providers (TLS 1.3 minimum)
- Anonymization/pseudonymization where feasible
- Regular audits of data flows to AI systems
- Implementation of data retention policies (local system only)
- Technical measures to prevent inadvertent data use for training

4.4 Provider Management

- Maintain current Data Processing Agreements with Groq and Cloudflare
- **Explicit contractual clauses prohibiting model training on our data**
- Regular verification of providers' no-storage commitments
- Annual security assessments of provider compliance
- Immediate termination rights if training on user data is discovered
- Contingency plans for provider changes or failures

4.5 User Data Rights

Ensure users can exercise:

- Right to access AI-processed data
- Right to correction of AI-generated content
- Right to deletion (where applicable)
- Right to object to AI processing

- Right to human review of AI decisions
- **Right to guarantee their data is not used for training**

5. Human Oversight Framework

5.1 Oversight Mechanisms

- **Pre-deployment Review**: Human validation of AI features before release
- **Runtime Monitoring**: Real-time monitoring of AI outputs for anomalies using user ratings
- **User Override**: Users maintain full control to modify or reject AI suggestions and content
- **Escalation Procedures**: Clear paths for users to request human intervention via

5.2 Human-in-the-Loop Requirements

- Critical decisions must allow for human review
- Users must be able to understand AI suggestions
- Clear options to disable AI features
- Regular human audits of AI performance

5.3 Staff Training

- Annual training on EU AI Act requirements
- Role-specific training for developers and support staff
- Documentation of training completion
- Regular updates on regulatory changes

6. Technical and Organizational Measures

6.1 Security Measures

- Access logging and monitoring
- Incident response procedures for AI-related security events
- Regular penetration testing of AI integrations

6.2 Quality Assurance

- Automated testing of AI features
- Performance benchmarking against quality metrics
- Regular accuracy assessments
- Manual quality review of all BETA features before full availability

6.3 System Reliability

- Service level monitoring for AI providers
- Fallback mechanisms for AI service failures
- Backup providers or degraded mode operations
- Regular disaster recovery testing

7. Compliance Monitoring and Reporting

7.1 Internal Compliance Monitoring

- Annual compliance checks against this framework
- Annual management reviews
- Annual comprehensive compliance audits
- Continuous monitoring of regulatory updates

7.3 External Reporting

- Regulatory notifications as required
- Stakeholder communications on significant changes
- Public documentation updates e.g. processor lists etc.

8. AI Specific Third-Party Provider Management

The following applies in addition to the existing Third-Party Management Policy

8.1 Provider Requirements

- Contractual commitments to no data storage
- **Explicit prohibition on training models with SlideHub user data**
- **Written guarantees that no user content enters training pipelines**
- EU data protection compliance
- Security certifications (ISO 27001 or equivalent)
- Transparency about AI model updates
- Incident notification agreements
- Audit rights to verify no-training commitments

8.2 Provider Monitoring

- Annual reviews of provider compliance
- **Regular audits to verify no training on user data**
- Annual security assessments
- Performance benchmarking
- Alternative provider evaluation
- Monitoring of provider public statements about training data

8.3 Change Management

- Impact assessment for provider changes
- User notification procedures
- Data migration protocols (if applicable)
- Continuity planning

9. Documentation and Record Keeping

9.1 Required Documentation

- This compliance framework and updates
- Risk assessments and mitigation measures
- Technical documentation of AI implementations
- Training records and certifications

- Incident logs and responses
- Audit reports and findings
- Provider agreements and assessments

9.2 Retention Periods

- Compliance documentation: 5 years minimum
- Incident records: 3 years
- Training records: 3 years
- Audit reports: 5 years
- Risk assessments: 5 years or until superseded

9.2 Review and Update Procedures

- Annual review of entire framework
- Quarterly updates for regulatory changes
- Ad-hoc updates for significant incidents
- Version control and change documentation

10. Contact Information

AI Compliance Officer
Email: anders.thomsen@slidehub.com

Data Protection Officer
Email: privacy@slidehub.com

Version	Date	Description	Creator	Approval by
1	Sep 18, 2025	The initial version of the policy	Anders Thomsen	Lasse Petersen
1.2	Sep 29, 2025	Updated version	Eerika Kuurne	Anders Thomsen
1.3	Feb 6, 2026	Updated version	Eerika Kuurne	Lasse Petersen