# Contents

**SLA a DPA požadavky u poskytovatelů AI API** **1**
1. Service Level Agreement (SLA) požadavky . . . 1
1.1 Dostupnost služby (Availability) . . . 1
1.2 Performance metriky . . . 2
1.3 Data Processing SLA . . . 2
2. Data Processing Agreement (DPA) požadavky . . . 2
2.1 Právní základ a role . . . 2
2.2 Data residency a transfers . . . 2
2.3 Subprocessors management . . . 2
3. Security Requirements . . . 2
3.1 Technical safeguards . . . 2
3.2 Organizational measures . . . 3
3.3 Audit and compliance . . . 3
4. Incident Response a Business Continuity . . . 3
4.1 Incident categories . . . 3
4.2 Communication requirements . . . 3
4.3 Business Continuity Plan . . . 3
5. Contractual Terms . . . 4
5.1 Liability and indemnification . . . 4
5.2 Insurance requirements . . . 4
5.3 Termination and data return . . . 4
6. Monitoring a Reporting . . . 4
6.1 Regular reporting . . . 4
6.2 Real-time monitoring . . . 4
7. Compliance Documentation . . . 4
7.1 Required certifications . . . 4
7.2 Documentation requirements . . . 5

# SLA a DPA požadavky u poskytovatelů AI API

**Verze:** 1.0
**Platnost od:** [DATUM]
**Příloha k:** AI Usage Policy
**Účel:** Standardizace smluvních požadavků na AI poskytovatele

## 1. Service Level Agreement (SLA) požadavky

### 1.1 Dostupnost služby (Availability)

**Minimální požadavky:** - **Uptime:** 99.9% měsíčně (max. 43 minut výpadku za měsíc) - **Planned maintenance:** Max. 4 hodiny měsíčně s 48h předchozím oznámením - **Emergency maintenance:** Max. 2 hodiny bez předchozího oznámení

**Penalties za nedodržení:** - 99.5-99.9%: 10% credit z měsíčního poplatku - 99.0-99.5%: 25% credit z měsíčního poplatku - Pod 99.0%: 50% credit + právo na okamžité vypovězení smlouvy

### 1.2 Performance metriky

**Response Time:** - API calls: 95% pod 2 sekundy, 99% pod 5 sekund - Batch processing: Definováno podle velikosti requestu - Error rate: Max. 0.5% failed requests za hodinu

**Throughput:** - Guaranteed minimum requests per minute podle tarifu - Burst capability: Min. 2x normal throughput na 5 minut - Rate limiting transparentní s HTTP 429 responses

### 1.3 Data Processing SLA

**Data retention:** - Input data: Max. 30 dní (nebo kratší podle DPA) - Logs: Max. 90 dní pro debugging purposes - Backups: Podle retention policy v DPA

**Data deletion:** - Na požádání: Do 30 dní - Při vypovězení smlouvy: Do 60 dní s potvrzením - Regular purging: Automaticky podle retention policy

## 2. Data Processing Agreement (DPA) požadavky

### 2.1 Právní základ a role

**Controller vs. Processor:** - AI vendor je data processor, klient je data controller - Jasně definované instructions pro zpracování - Prohibition na použití dat pro vlastní účely (training, improvement)

**Purpose limitation:** - Data zpracovávána pouze pro poskytnutí AI služby - Žádné secondary use bez explicit consent - Žádné data mining nebo profiling bez souhlasu

### 2.2 Data residency a transfers

**EU Data Residency:** - Všechna data zpracovávána v EU datacenters - Lista konkrétních zemí a datacenter lokací - Prohibition na transfer mimo EU bez adequate protection

**International transfers (pokud nutné):** - Standard Contractual Clauses (SCC) 2021 version - Transfer Impact Assessment (TIA) dokumentace - Additional safeguards podle konkrétní země

### 2.3 Subprocessors management

**Subprocessor approval process:** - Lista všech current subprocessors s rolemi - 30-day prior notice pro nové subprocessors - Right to object s alternative solution

**Subprocessor requirements:** - Same data protection obligations jako main processor - Regular audits a compliance monitoring - Immediate notification při změnách compliance status

## 3. Security Requirements

### 3.1 Technical safeguards

**Encryption:** - Data in transit: TLS 1.3 minimum - Data at rest: AES-256 nebo equivalent - Key management: HSM nebo equivalent with proper rotation

**Access controls:** - Multi-factor authentication for all admin access - Role-based access control (RBAC) - Regular access reviews (quarterly minimum) - Segregation of duties pro sensitive operations

### 3.2 Organizational measures

**Staff training:** - Regular data protection training pro všechny employeesy - Confidentiality agreements s penalty clauses - Background checks pro personnel s přístupem k datům

**Incident management:** - 24/7 security monitoring - Incident response plan s definovanými timeframes - Client notification do 72 hodin při personal data breach

### 3.3 Audit and compliance

**Regular audits:** - SOC 2 Type II annual audit (current certificate required) - ISO 27001 certification (current certificate required) - GDPR compliance audit (annual nebo při změnách)

**Penetration testing:** - External penetration testing minimálně yearly - Vulnerability assessments quarterly - Results sharing s klientem (executive summary minimum)

## 4. Incident Response a Business Continuity

### 4.1 Incident categories

**Severity 1 (Critical):** - Service completely unavailable - Data breach s personal data - Security incident s potential data exposure - Response time: 1 hodina, resolution target: 4 hodiny

**Severity 2 (High):** - Significant performance degradation - Partial service unavailability - Security vulnerability discovered - Response time: 4 hodiny, resolution target: 24 hodin

### 4.2 Communication requirements

**Incident notification:** - Initial notification do 1 hodiny (Sev 1) nebo 4 hodin (Sev 2) - Hourly updates během critical incidents - Post-incident report do 5 business days

**Communication channels:** - Primary: Dedicated incident email/portal - Secondary: Phone contact pro Severity 1 - Escalation matrix s management contacts

### 4.3 Business Continuity Plan

**Disaster recovery:** - RTO (Recovery Time Objective): Max. 4 hodiny - RPO (Recovery Point Objective): Max. 1 hodina data loss - Geographic redundancy across multiple EU regions

**Backup and recovery:** - Daily incremental backups - Weekly full backups s retention podle DPA - Recovery testing quarterly s dokumentací results

## 5. Contractual Terms

### 5.1 Liability and indemnification

**Limitation of liability:** - No limitation pro data protection violations - No limitation pro security breaches caused by vendor negligence - General liability cap: 12x monthly fees nebo €1M, co je vyšší

**Indemnification:** - Vendor indemnifies klient pro third-party claims z data protection violations - Vendor indemnifies pro IP infringement claims - Mutual indemnification pro general negligence

### 5.2 Insurance requirements

**Cyber liability insurance:** - Minimum coverage: €5M pro Severity 1 vendors - Policy must cover data breach costs, regulatory fines - Certificate of insurance provided annually

**Professional indemnity:** - Minimum coverage: €2M - Covers errors and omissions v service delivery - Extended reporting period option

### 5.3 Termination and data return

**Termination triggers:** - Material breach s 30-day cure period - Insolvency nebo change of control bez approval - Failure to maintain required certifications

**Data return process:** - All data returned v machine-readable format do 60 days - Secure deletion from all systems včetně backups - Certificate of destruction provided

## 6. Monitoring a Reporting

### 6.1 Regular reporting

**Monthly reports:** - SLA performance metrics (uptime, response time, errors) - Security incidents summary - Capacity utilization a forecasting

**Quarterly reports:** - Compliance status update - Subprocessor changes - Risk assessment update

### 6.2 Real-time monitoring

**API monitoring:** - Response time monitoring s alerting - Error rate tracking - Capacity utilization monitoring

**Security monitoring:** - Access logging a anomaly detection - Failed authentication attempts - Unusual usage patterns

## 7. Compliance Documentation

### 7.1 Required certifications

**Current certificates required:** - SOC 2 Type II (valid, not older than 12 months) - ISO 27001 (valid) - GDPR compliance certification (když available)

**Additional certifications (preferred):** - ISO 42001 pro AI systems - FedRAMP nebo equivalent government certification - Industry-specific certifications (pokud applicable)

### 7.2 Documentation requirements

**Technical documentation:** - Data flow diagrams - Security architecture documentation - API documentation včetně security controls

**Legal documentation:** - Privacy policy a terms of service - DPA template - Subprocessor agreements template

---

**Template připraven:** RRSoft AI Technologies
**Pro použití:** Enterprise AI governance
**Konzultace doporučena:** Legal a IT security týmy

*Tento template přizpůsobte podle specifických potřeb vaší organizace a právní jurisdikce.*