Směrnice pro práci s daty v AI nástrojích (AI Data Handling Policy)

Verze: 1.0
Platnost od: [DATUM]
Příloha k: AI Usage Policy
Compliance: GDPR, NIS2, ISO/IEC 42001

1. Klasifikace dat pro AI zpracování

VEŘEJNÁ DATA (Public)

Definice: Data dostupná veřejnosti bez omezení
AI zpracování: Povoleno všemi schválenými nástroji
Příklady: - Publikované ceníky a nabídky - Veřejné prezentace a tiskové zprávy - Otevřená data z veřejných zdrojů - Veřejně dostupné právní dokumenty

Kontrolní otázky: - Je tento obsah dostupný na našem webu? - Lze jej najít pomocí vyhledávačů? - Neobsahuje žádné citlivé informace?

INTERNÍ DATA (Internal)

Definice: Data určená pouze pro interní použití organizace
AI zpracování: Pouze enterprise nástroje s DPA a EU hosting
Příklady: - Interní dokumentace a procesy - Neveřejné prezentace pro management - Aggregované statistiky (anonymizované) - Obecné projektové informace

Povinné kontroly: - Enterprise nástroj s podepsanou DPA - Data residency v EU - Audit trail a logging - Schválení nadřízeného

DŮVĚRNÁ DATA (Confidential)

Definice: Citlivá obchodní data s omezením přístupu
AI zpracování: Pouze po speciálním schválení + on-premises
Příklady: - Strategické plány a roadmapy - Finanční výsledky (před publikováním) - Významné obchodní smlouvy - Technické specifikace produktů

Approval proces: 1. Žádost přes [GOVERNANCE-COMMITTEE@COMPANY.COM] 2. Hodnocení Legal + IT Security + Business owner 3. Písemné schválení + monitorování použití 4. Časové omezení přístupu (max. 30 dní)

VYSOCE CITLIVÁ DATA (Restricted)

Definice: Data podléhající zvláštní ochraně
AI zpracování: ZAKÁZÁNO bez výjimky
Příklady: - Osobní údaje fyzických osob - Zdravotní a biometrické údaje - Finanční údaje klientů - Hesla, API klíče, certifikáty - Právnicky privilegované komunikace

2. Technická opatření

2.1 Pseudonymizace a anonymizace

Před nahráním do AI:

```
Původní data: "Pan Novák z firmy ABC s.r.o. má dluh 150,000 Kč"
Pseudonymizovaná: "Klient #12345 z firmy [COMPANY-B] má dluh [AMOUNT] Kč"
```

`Anonymizovaná: "Průměrný dluh v segmentu SMB: 150,000 Kč"`

Nástroje pro anonymizaci: - Microsoft Presidio (open-source PII detection) - Interno custom scripts pro data masking - Manual review před odesláním citlivých dat

2.2 Data retention management

Automatické mazání: - Chat historie AI nástrojů: 90 dní - Temporary files a uploads: 30 dní - AI-generated outputs: 12 měsíců (s audit trail)

Manual retention: - Strategicky důležité AI výstupy: dokumentovat důvod - Business-critical analýzy: schválení legal týmu - Training data pro custom models: special retention policy

2.3 Monitoring a audit trail

Co monitorujeme: - Kdo použil AI nástroj (user ID, timestamp) - Jaký typ dat byl nahrazen (classification level) - Který nástroj byl použit (vendor, model version) - Výstup byl export nebo delete

Automatické alerting: - Upload confidential/restricted dat → okamžité upozornění - Anomálie v usage patterns → týdenní report - Failed authentication → real-time alert

3. Procedury pro konkrétní scénáře

3.1 Analýza dokumentů s osobními údaji

KROK 1: Data assessment - Identifikace typů osobních údajů - DPIA (Data Protection Impact Assessment) pokud nutné - Legal basis podle GDPR čl. 6

KROK 2: Anonymizace

```
# Příklad preprocessing scriptu
sed 's/[0-9]\{9,\}/[ID-MASKED]/g' | \
sed 's/[a-zA-Z0-9._%+-]\+@[a-zA-Z0-9.-]\+\.[a-zA-Z]\{2,\}/[EMAIL-MASKED]/g' | \
sed 's/[0-9]\{3\} [0-9]\{3\} [0-9]\{3\}/[PHONE-MASKED]/g'
```

KROK 3: AI processing - Pouze enterprise nástroje s GDPR compliance - Dokumentace zpracování (čl. 30 GDPR) - Retention period: max. 6 měsíců

3.2 Finanční analýzy a reporting

Před AI zpracováním: - Agregace na vyšší úrovni (ne individual transactions) - Removal of identifiable information - Legal review pro sensitive financial metrics

AI použití: - Trend analysis, forecasting models - Risk assessment (aggregated data only) - Compliance reporting (anonymized data)

Po AI zpracování: - Double-check na data leakage - Management review před finalizací - Archive with proper classification

3.3 HR data a performance reviews

ČISTĚ ZAKÁZÁNO pro externí AI: - Individual performance data - Salary information - Disciplinary records - Personal development plans

Povoleno pouze pro aggregated analytics: - Anonymizované satisfaction surveys - Department-level productivity metrics - General skills gap analysis

4. Incident response procedures

4.1 Suspected data breach

OKAMŽITĚ (do 1 hodiny): 1. Kontakt: [DATA-BREACH-TEAM@COMPANY.COM] 2. Screenshot/evidence collection 3. Immediate containment (block access if needed) 4. Initial impact assessment

DO 24 HODIN: 1. Detailed forensic analysis 2. Notification příslušných autorit (ÚOOÚ) 3. Communication plan pro affected stakeholders 4. Remediation action plan

4.2 Accidental exposure

Okamžité akce: - Pause/stop AI processing - Document what data was exposed - Check if data was stored/cached by AI service - Request deletion from AI vendor

Follow-up: - Internal investigation a lessons learned - Policy update pokud je potřeba - Additional training pro involved parties

5. Vendor management a due diligence

5.1 New AI tool evaluation

Security checklist: - [ ] SOC 2 Type II certification - [ ] ISO 27001 certification - [ ] GDPR compliance documentation - [ ] Data processing agreement (DPA) - [ ] EU data residency options - [ ] Security incident history review - [ ] Data retention a deletion capabilities

Legal checklist: - [ ] Terms of service review - [ ] Data licensing rights - [ ] Liability a insurance coverage - [ ] Intellectual property provisions - [ ] Termination a data return procedures

5.2 Ongoing vendor monitoring

Quarterly reviews: - Security posture updates - Terms of service changes - New data processing locations - Incident reports a response

Annual audits: - Comprehensive security assessment - DPA compliance verification - Cost-benefit analysis - Alternative vendor evaluation

6. Training a awareness

6.1 Role-based training

All employees: - Basic data classification - Prohibited use cases - How to report incidents

AI power users: - Advanced anonymization techniques - Vendor-specific security controls - Data handling best practices

IT administrators: - Technical implementation details - Monitoring a alerting setup - Incident response procedures

6.2 Regular updates

Monthly: Security awareness newsletter
Quarterly: Policy updates a changes
Annually: Comprehensive refresher training

Otázky a clarifications: [DATA-GOVERNANCE@COMPANY.COM]

Tento dokument je living document a bude pravidelně aktualizován na základě nových regulations a business needs.