| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem zadajte názov registrovanej právnickej osoby | | | | | | | |
| Číslo dokumentu:<br>P16 | | | | | Názov dokumentu:<br>**Politika maskovania údajov a pseudonymizácie P16S** | | | | | | | |
| Verzia:<br>1.0 | | Dátum nadobudnutia účinnosti:<br>01.01.2025 | | | Vlastník dokumentu: | | | | | | | |
| X | Politika | | Štandard | | Postup | | Formulár | | Register | | Iné | |

| **História revízií** | | | | |
|---|---|---|---|---|
| **Číslo revízie** | **Dátum revízie** | **Zmeny** | **Preskúmal** | **Vlastník procesu** |
| | | | | |
| | | | | |

| **Schválenia** | | | |
|---|---|---|---|
| **Meno** | **Pozícia** | **Dátum** | **Podpis** |
| | | | |
| | | | |

Súlad s normami a predpismi

| Norma/predpis | Kapitola/článok | Poznámka |
|---|---|---|
| ISO/IEC 27001:2022 | Kapitola 6.1 | Všeobecné požiadavky na riadenie rizík a prevádzkové kontroly pre maskovanie údajov a pseudonymizáciu |
| ISO/IEC 27002:2022 | Kontroly 8.11, 8 | Usmernenia ku kontrolám na implementáciu maskovania údajov a pseudonymizácie |
| NIST SP 800-53 Rev.5 | PM-17, PT-2, PT-3, SC-12, SC-28, SC-30 | Kontroly ochrany súkromia a dôvernosti na minimalizáciu údajov, transformáciu a obmedzenie prístupu |
| Nariadenie EÚ GDPR | Články 4 ods. 5, 5 ods. 1 písm. c), f), 32 | Právny základ a požiadavky na pseudonymizáciu a opatrenia na ochranu údajov |
| Smernica EÚ NIS2 | Článok 21 ods. 2 písm. c) | Povinnosť zaviesť technické a organizačné opatrenia vrátane technológií na posilnenie ochrany súkromia (PET) |
| Nariadenie EÚ DORA | Články 10 ods. 1, 10 ods. 2 písm. e) | Riadenie rizík IKT a kontroly dôvernosti pre maskovanie údajov a pseudonymizáciu |
| COBIT 2019 | DSS05.01, DSS06.06, MEA | Kontroly správy a riadenia na ochranu údajov prostredníctvom maskovania a na posudzovanie súladu |

**1. Účel**

1.1 Táto politika stanovuje prístup organizácie k implementácii maskovania údajov a pseudonymizácie ako technológií na posilnenie ochrany súkromia (PET) s cieľom znížiť identifikovateľnosť a vystavenie osobných alebo citlivých údajov.

1.2 Podporuje bezpečné používanie informácií pri testovaní, analytike a prevádzke pri súčasnom dodržiavaní zákonných a regulačných požiadaviek, zmierňovaní dôsledkov porušenia ochrany údajov a uplatňovaní zásad minimalizácie údajov a dôvernosti.

1.3 Táto politika je v súlade s ISO/IEC 27001:2022, podporuje článok 4 ods. 5 GDPR týkajúci sa pseudonymizácie a integruje implementáciu založenú na riziku v súlade s normami NIST, NIS2, DORA a COBIT 2019.

**2. Rozsah**

**2.1 Táto politika sa vzťahuje na:**

2.1.1 všetkých zamestnancov, zmluvných pracovníkov, tretie strany a dodávateľov s prístupom k systémom, ktoré spracúvajú osobné, dôverné alebo citlivé informácie,

2.1.2 všetky dátové prostredia vrátane produkčného, vývojového, testovacieho a predprodukčného prostredia,

2.1.3 všetky formy maskovania údajov (napr. statické, dynamické, deterministické, tokenizácia) a techniky pseudonymizácie používané na zníženie rizík pre súkromie,

2.1.4 všetky typy údajov (štruktúrované aj neštruktúrované), systémy (vo vlastnej infraštruktúre alebo v cloudovom prostredí) a aplikácie zahŕňajúce osobné údaje alebo údaje podliehajúce regulácii.

**2.2 Rozsah zahŕňa použitie v:**

2.2.1 prostrediach vývoja aplikácií a QA/testovania,

2.2.2 analytických alebo reportovacích platformách,

2.2.3 výmene údajov s tretími stranami alebo poskytovateľmi služieb,

2.2.4 zálohovacích, archivačných alebo obnovovacích systémoch.

**3. Ciele**

3.1 Zabezpečiť konzistentné a účinné uplatňovanie maskovania údajov a pseudonymizácie na zníženie rizika vystavenia údajov alebo ich zneužitia.

3.2 Zabezpečiť, aby sa skutočné údaje nikdy nepoužívali v neprodukčných prostrediach, pokiaľ neboli transformované pomocou schválených techník PET.

3.3 Zachovať referenčnú integritu, použiteľnosť a transformácie zachovávajúce formát, ak sa vyžadujú na zabezpečenie prevádzkovej konzistentnosti.

3.4 Uplatňovať prísne riadenie prístupu k pôvodným údajom, maskovaným údajom a kľúčom na opätovnú identifikáciu.

3.5 Považovať maskované alebo pseudonymizované dátové súbory za citlivé údaje, na ktoré sa vzťahuje auditné logovanie, kontroly uchovávania a postupy reakcie na incidenty.

3.6 Overovať účinnosť týchto kontrol prostredníctvom priebežného testovania, monitorovania a auditných postupov.

**4. Roly a zodpovednosti**

**4.1 Vrcholový manažment**

4.1.1 Schvaľuje túto politiku a zabezpečuje jej uplatňovanie ako súčasť širších iniciatív v oblasti správy a riadenia IT a ochrany údajov.

**4.2 Riaditeľ informačnej bezpečnosti (CISO) / manažér ISMS**

4.2.1 Dohliada na implementáciu a priebežný súlad.

4.2.2 Zabezpečuje súlad s ISO/IEC 27001, kapitolou 6.1.3 (ošetrenie rizík) a kapitolou 8.1 (prevádzkové kontroly).

4.2.3 Preskúmava auditné logy a overuje účinnosť kontrol.

[ ... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ... ]

**9. Požiadavky na preskúmanie a aktualizáciu**

**9.1 Táto politika sa musí preskúmať najmenej raz ročne alebo skôr v prípade:**

9.1.1 regulačných zmien ovplyvňujúcich maskovanie údajov alebo pseudonymizáciu,

9.1.2 zavedenia nových IT systémov spracúvajúcich citlivé údaje,

9.1.3 významných zmien v schéme klasifikácie údajov organizácie,

9.1.4 auditných zistení poukazujúcich na nedostatky kontrol,

9.1.5 výskytu nových hrozieb alebo technológií maskovania.

9.2 Manažér ISMS vedie preskúmanie po konzultácii s DPO, vlastníkmi údajov, IT bezpečnosťou a právnym oddelením. Aktualizácie musia podliehať riadeniu verzií, byť schválené vrcholovým manažmentom a oznámené všetkým dotknutým zainteresovaným stranám.

## 10. Súvisiace politiky a väzby

10.1 P13 - Politika klasifikácie a označovania údajov. Rozhodnutia o maskovaní údajov a pseudonymizácii sú priamo závislé od klasifikácie dátových polí a úrovní citlivosti definovaných v P13.

10.2 P14 - Politika uchovávania a likvidácie údajov. Transformované dátové súbory sa musia uchovávať a likvidovať v súlade s pravidlami životného cyklu uvedenými v P14, pričom sa zabezpečí, aby sa s maskovanými a pseudonymizovanými údajmi zaobchádzalo ako s citlivými údajmi.

10.3 P17 - Politika ochrany údajov a súkromia. Poskytuje zásady ochrany súkromia a regulačné východiská pre uplatňovanie pseudonymizácie ako činnosti spracúvania v súlade s GDPR a obdobnými právnymi predpismi.

10.4 P22 - Politika logovania a monitorovania. Umožňuje centralizovaný audit a generovanie upozornení pre udalosti maskovania údajov a pseudonymizácie v súlade so štruktúrovanými postupmi bezpečnostného monitorovania.

## 11. Referenčné normy a rámce

### 11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1.3 - plán ošetrenia rizík: stanovuje maskovanie údajov a pseudonymizáciu ako mechanizmy ošetrenia rizík na zníženie identifikovateľnosti citlivých údajov v prostrediach spracúvania, ktoré nie sú nevyhnutné pre produkciu.

11.1.2 Kapitola 8.1 - prevádzkové plánovanie a riadenie: ukladá technické a procedurálne kontroly pre bezpečnú transformáciu údajov počas spracúvania, uchovávania alebo prenosu.

### 11.2 ISO/IEC 27002:2022

11.2.1 Kontroly 8.11, 8: usmernenia pre maskovanie údajov a pseudonymizáciu s cieľom minimalizovať riziká opätovnej identifikácie a úniku údajov.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - ochrana PII: implementácia technológií na posilnenie ochrany súkromia, ako sú maskovanie údajov a pseudonymizácia.

11.3.2 PT-2, PT-3: minimalizácia a bezpečnosť spracúvania PII - transformácia na zníženie identifikovateľnosti a uplatňovanie riadenia prístupu.

11.3.3 SC-12, SC-28, SC-30: dôvernosť a integrita údajov - kontroly dôvernosti a zastretia pri uchovávaní, prenose a používaní.

### 11.4 Nariadenie EÚ GDPR (2016/679)

11.4.1 Článok 4 ods. 5: formálna definícia pseudonymizácie.

11.4.2 Článok 32: bezpečnosť spracúvania - organizačné a technické opatrenia pre pseudonymizáciu.

11.4.3 Článok 5 ods. 1 písm. c), f): minimalizácia údajov a dôvernosť prostredníctvom pseudonymizácie/maskovania údajov.

### 11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21 ods. 2 písm. c): vyžaduje technológie PET, ako sú maskovanie údajov a pseudonymizácia, ako bezpečnostné opatrenia.

### 11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 10 ods. 1: rámec riadenia rizík IKT zahŕňa kontroly maskovania údajov/pseudonymizácie.

11.6.2 Článok 10 ods. 2 písm. e): ukladá používanie transformačných technológií na ochranu osobných a finančných údajov.

### 11.7 COBIT 2019

11.7.1 DSS05.01: chrániť informačné aktíva - požiadavky na maskovanie údajov a pseudonymizáciu.

11.7.2 DSS06.06: bezpečné testovanie a analytika - maskovanie údajov v neprodukčných prostrediach.

11.7.3 MEA03: monitorovanie súladu z hľadiska účinnosti maskovania údajov a pseudonymizácie.