					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P16S					Názov dokumentu: **Politika maskovania údajov a pseudonymizácie P16S**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 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 6.1.3, Kapitola 8	Riziká informačnej bezpečnosti a nevyhnutné kontroly vrátane maskovania a pseudonymizácie
ISO/IEC 27002:2022	Kontroly 8.11, 8.12	Usmernenie k maskovaniu a predchádzaniu úniku údajov
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Zneprehľadnenie údajov, technológie na zvýšenie ochrany súkromia
EÚ NIS2	Článok 21(2)(c)	Primerané technické opatrenia, pseudonymizácia ako kontrola
EÚ DORA	Článok 10(1)	Kontroly rizík IKT vrátane ochranných opatrení pri transformácii
COBIT 2019	DSS05.01, DSS06	Ochrana údajov, techniky zneprehľadnenia a pseudonymizácie
EÚ GDPR	Články 4(5), 5(1)(c), 32	Minimalizácia údajov, pseudonymizácia ako technická kontrola

1. Účel

1.1. Táto politika stanovuje záväzné požiadavky na používanie maskovania údajov a pseudonymizácie na ochranu citlivých, osobných a dôverných údajov v malých a stredných podnikoch (MSP).

1.2. Tieto techniky sa musia používať všade tam, kde nie sú potrebné reálne údaje, napríklad pri vývoji, analytike alebo v scenároch poskytovania služieb tretími stranami, a prispievajú k zníženiu rizika sprístupnenia, zneužitia alebo porušenia ochrany údajov.

1.3. Táto politika priamo podporuje súlad s požiadavkami certifikácie podľa ISO/IEC 27001:2022, ako aj s európskymi regulačnými požiadavkami, ako sú GDPR, smernica EÚ NIS2 a nariadenie EÚ DORA.

1.4. Transformáciou údajov pred ich použitím mimo pôvodného prevádzkového kontextu organizácia obmedzuje svoju zodpovednosť a zvyšuje schopnosť preukázať náležitú starostlivosť v oblasti ochrany súkromia a bezpečnosti.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetky štruktúrované aj neštruktúrované údaje klasifikované ako osobné, dôverné alebo citlivé, bez ohľadu na to, či sú uchovávané alebo spracúvané:

2.1.1. v produkčnom, testovacom alebo vývojovom prostredí,

2.1.2. na lokálnych zariadeniach, serveroch alebo cloudových platformách,

2.1.3. internými pracovníkmi, zmluvnými pracovníkmi alebo poskytovateľmi tretích strán.

2.2. Vzťahuje sa aj na všetky nástroje na transformáciu údajov (maskovanie, tokenizácia, pseudonymizácia), bez ohľadu na to, či sú open source, komerčné alebo vyvinuté interne.

2.3. Prípady použitia podľa tejto politiky zahŕňajú:

2.3.1. prípravu testovacích alebo vývojových dátových súborov,

2.3.2. export údajov do analytických systémov,

2.3.3. prístup dodávateľov alebo konzultantov do prevádzkových systémov,

2.3.4. minimalizáciu údajov dotknutých osôb na zníženie rizika spracúvania.

3. Ciele

3.1. Zabezpečiť, aby reálne osobné alebo citlivé údaje nikdy neboli sprístupnené v prostrediach s nižšou úrovňou bezpečnosti, kde nie sú nevyhnutné.

3.2. Stanoviť povinnosť používať maskovanie alebo pseudonymizáciu vždy, keď na vykonanie úlohy nie sú striktne potrebné skutočné identifikátory.

3.3. Predchádzať neoprávnenému prístupu k údajom alebo ich zneužitiu tým, že sa pred prenosom alebo spracúvaním uplatnia kontroly transformácie.

3.4. Zabezpečiť, aby všetky procesy maskovania a pseudonymizácie boli sledovateľné, auditovateľné a vykonávané prostredníctvom schválených nástrojov.

3.5. Zabezpečiť súlad s príslušnými právnymi a regulačnými požiadavkami na minimalizáciu údajov, dôvernosť a ochranné opatrenia pri transformácii.

4. Roly a zodpovednosti

4.1. Generálny manažér (GM)

4.1.1. je vlastníkom tejto politiky a schvaľuje ju,

4.1.2. zabezpečuje, aby všetky oddelenia a poskytovatelia dodržiavali požiadavky na transformáciu údajov,

4.1.3. preskúmava výnimky, posúdenia rizík a logy transformácie,

4.1.4. koordinuje právne, prevádzkové alebo dodávateľské opatrenia v prípade porušení.

4.2. Poskytovateľ IT podpory / interné IT

4.2.1. vyberá a spravuje nástroje na maskovanie alebo pseudonymizáciu,

4.2.2. zabezpečuje uplatnenie vhodných metód transformácie podľa typu údajov,

4.2.3. vedie logy transformovaných dátových súborov a postupov správy kľúčov,

4.2.4. zabezpečuje, aby sa maskovanie vykonalo pred použitím na testovanie, pre dodávateľov alebo na analytiku.

[... 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. Ročné preskúmanie

9.1.1. Túto politiku musí generálny manažér preskúmať najmenej raz ročne, aby sa zabezpečilo, že zohľadňuje:

9.1.1.1. aktualizácie príslušných predpisov (napr. GDPR, DORA),

9.1.1.2. nové podnikové systémy alebo výmenu údajov s tretími stranami,

9.1.1.3. spätnú väzbu z auditov alebo incidentov súvisiacich s používaním nemaskovaných údajov.

9.2. Mimoriadne preskúmania

9.2.1. Preskúmania sa musia vykonať aj vtedy, keď:

9.2.1.1. sú zavedené nové aplikácie alebo platformy, ktoré spracúvajú citlivé údaje,

9.2.1.2. závažný incident odhalí medzery v aktuálnych kontrolách transformácie,

9.2.1.3. zmeny klasifikačných úrovní ovplyvnia postupy nakladania s údajmi.

9.3. Riadenie verzií a zmien

9.3.1. Všetky zmeny politiky musia byť:

9.3.1.1. schválené GM a zdokumentované v zozname zmien,

9.3.1.2. jasne oznámené dotknutým zamestnancom a poskytovateľom služieb,

9.3.1.3. bezpečne archivované s obmedzeným prístupom k neaktuálnym verziám.

10. Súvisiace politiky a väzby

10.1. Táto politika sa musí uplatňovať spolu s nasledujúcimi politikami SME, aby sa zabezpečila konzistentná a záväzná ochrana citlivých údajov:

10.1.1. P13S – Politika klasifikácie a označovania údajov: Definuje klasifikačné úrovne (napr. „Dôverné – osobné“), ktoré určujú, kedy sa musí uplatniť maskovanie alebo pseudonymizácia. Táto politika presadzuje pravidlá transformácie podľa úrovne citlivosti údajov.

10.1.2. P14S – Politika uchovávania a likvidácie údajov: Zabezpečuje, aby sa transformované dátové súbory vrátane záloh obsahujúcich maskované alebo pseudonymizované údaje uchovávali a likvidovali podľa príslušných pravidiel vrátane odstránenia mapovacích kľúčov, keď už nie sú potrebné.

10.1.3. P17S – Politika ochrany údajov a súkromia: Zosúlaďuje postupy transformácie so širšími povinnosťami v oblasti ochrany súkromia vrátane požiadaviek GDPR na minimalizáciu údajov a používanie pseudonymizácie ako ochranného opatrenia pri spracúvaní osobných údajov.

10.1.4. P30S – Politika reakcie na incidenty: Upravuje postupy nahlasovania a eskalácie v prípade neoprávneného sprístupnenia údajov vrátane nesprávneho použitia alebo reverzie maskovaných alebo pseudonymizovaných údajov.

10.1.5. P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: Priraďuje celkovú zodpovednosť za implementáciu politiky, akceptáciu rizika a schvaľovanie výnimiek, predovšetkým generálnemu manažérovi.

10.2. Tieto politiky tvoria integrovaný rámec ochrany údajov, ktorý zabezpečuje, že činnosti maskovania a pseudonymizácie podporujú certifikáciu podľa ISO 27001 a súlad s regulačnými požiadavkami.

11. Referenčné normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 6.1.3: Vyžaduje ošetrenie rizík informačnej bezpečnosti, čo zahŕňa aj zmierňovanie expozície prostredníctvom techník transformácie údajov.

11.1.2. Kapitola 8.1: Ukladá implementáciu kontrol potrebných na splnenie bezpečnostných cieľov vrátane pseudonymizácie a maskovania.

11.2. ISO/IEC 27002

11.2.1. Kontrola 8.11: Poskytuje usmernenie k maskovaniu citlivých údajov v testovacích a vývojových systémoch.

11.2.2. Kontrola 8.12: Poskytuje postupy na predchádzanie úniku údajov prostredníctvom riadenej transformácie a postupov riadenia prístupu.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Zabezpečuje dôvernosť informácií prostredníctvom zneprehľadnenia údajov.

11.3.2. SC-28: Chráni informácie v pokoji aj počas používania.

11.3.3. PT-2/PT-3: Podporujú používanie technológií na zvýšenie ochrany súkromia vrátane pseudonymizácie pri spracúvaní PII.

11.4. EÚ GDPR

11.4.1. Článok 4(5): Právne vymedzuje pseudonymizáciu a vyžaduje kontroly nad mapovacími kľúčmi a identifikátormi.

11.4.2. Článok 5(1)(c): Podporuje zásadu minimalizácie údajov prostredníctvom maskovania.

11.4.3. Článok 32: Uznáva pseudonymizáciu ako technickú kontrolu, ktorá znižuje riziká pre súkromie.

11.5. Smernica EÚ NIS2

11.5.1. Článok 21(2)(c): Vyžaduje primerané technické opatrenia na minimalizáciu rizika pre bezpečnosť údajov vrátane pseudonymizácie ako súčasti riadenia rizík.

11.6. Nariadenie EÚ DORA

11.6.1. Článok 10(1): Ukladá kontroly rizík súvisiacich s IKT vrátane ochranných opatrení pri transformácii údajov na zabezpečenie kontinuity a dôvernosti počas outsourcingu a vývoja systémov.

11.7. COBIT 2019

11.7.1. DSS05.01: Vyžaduje ochranu informačných aktív vrátane transformácie tam, kde je to možné.

11.7.2. DSS06.06: Vyžaduje primerané techniky zneprehľadnenia a pseudonymizácie na obmedzenie sprístupnenia údajov v prostrediach s nižšou úrovňou dôvery.