					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P16S					Název dokumentu: **Politika maskování dat a pseudonymizace**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma/právní předpis	Ustanovení/článek	Komentář
ISO/IEC 27001:2022	Článek 6.1.3, článek 8	Rizika bezpečnosti informací a nezbytná opatření, včetně maskování a pseudonymizace
ISO/IEC 27002:2022	Opatření 8.11, 8.12	Pokyny k maskování a prevenci úniku dat
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Zastření dat, technologie zvyšující ochranu soukromí
směrnice NIS2	Článek 21(2)(c)	Přiměřená technická opatření, pseudonymizace jako opatření
nařízení DORA	Článek 10(1)	Opatření pro řízení rizik v oblasti ICT, včetně ochranných mechanismů transformace
COBIT 2019	DSS05.01, DSS06	Ochrana dat, techniky zastření a pseudonymizace
GDPR	Články 4(5), 5(1)(c), 32	Minimalizace údajů, pseudonymizace jako technické opatření

1. Účel

1.1. Tato politika stanoví závazné požadavky na používání maskování dat a pseudonymizace za účelem ochrany citlivých, osobních a důvěrných údajů v malých a středních podnicích (SME).

1.2. Tyto techniky jsou povinné všude tam, kde skutečná data nejsou nezbytná, například při vývoji, analytice nebo v situacích zahrnujících poskytovatele služeb třetích stran, a pomáhají snižovat rizika zpřístupnění, zneužití nebo narušení bezpečnosti dat.

1.3. Tato politika přímo podporuje soulad s požadavky na certifikaci podle ISO/IEC 27001:2022 i s evropskými regulačními požadavky, jako jsou GDPR, směrnice NIS2 a nařízení DORA.

1.4. Transformací dat před jejich použitím mimo původní obchodní kontext organizace omezuje organizace svou odpovědnost a zvyšuje schopnost doložit náležitou péči v oblasti ochrany soukromí a bezpečnosti.

2. Rozsah

2.1. Tato politika se vztahuje na všechna strukturovaná i nestrukturovaná data klasifikovaná jako osobní, důvěrná nebo citlivá, bez ohledu na to, zda jsou ukládána nebo zpracovávána:

2.1.1. v produkčním, testovacím nebo vývojovém prostředí,

2.1.2. na lokálních zařízeních, serverech nebo cloudových platformách,

2.1.3. interním personálem, smluvními pracovníky nebo poskytovateli třetích stran.

2.2. Politika se rovněž vztahuje na všechny nástroje pro transformaci dat (maskování, tokenizaci, pseudonymizaci), a to bez ohledu na to, zda jsou open source, komerční nebo vyvinuté interně.

2.3. Případy použití podle této politiky zahrnují:

2.3.1. přípravu testovacích nebo vývojových datových sad,

2.3.2. export dat do analytických systémů,

2.3.3. přístup dodavatelů nebo konzultantů k provozním systémům,

2.3.4. minimalizaci údajů subjektů údajů za účelem snížení rizika zpracování.

3. Cíle

3.1. Zajistit, aby skutečné osobní nebo citlivé údaje nikdy nebyly zpřístupněny v prostředích s nižší úrovní zabezpečení, kde nejsou nezbytné.

3.2. Stanovit povinnost používat maskování nebo pseudonymizaci všude tam, kde skutečné identifikátory nejsou pro daný úkol bezpodmínečně nutné.

3.3. Zabránit neoprávněnému přístupu k datům nebo jejich zneužití prostřednictvím uplatňování transformačních opatření před přenosem nebo zpracováním dat.

3.4. Zajistit, aby všechny procesy maskování a pseudonymizace byly dohledatelné, auditovatelné a vynucované prostřednictvím schválených nástrojů.

3.5. Zajistit soulad s příslušnými právními a regulačními požadavky vyžadujícími minimalizaci údajů, důvěrnost a ochranná opatření založená na transformaci dat.

4. Role a odpovědnosti

4.1. generální ředitel (GM)

4.1.1. odpovídá za tuto politiku a schvaluje ji,

4.1.2. zajišťuje, aby všechna oddělení a poskytovatelé dodržovali požadavky na transformaci dat,

4.1.3. přezkoumává výjimky, hodnocení rizik a protokoly transformací,

4.1.4. koordinuje právní, provozní nebo dodavatelská opatření v případě porušení.

4.2. poskytovatel IT podpory / interní IT

4.2.1. vybírá a spravuje nástroje pro maskování nebo pseudonymizaci,

4.2.2. zajišťuje použití vhodných metod transformace podle typu dat,

4.2.3. vede protokoly transformovaných datových sad a postupů správy klíčů,

4.2.4. zajišťuje, aby k maskování došlo před použitím pro testování, dodavatele nebo analytiku.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1. Roční přezkum

9.1.1. Tato politika musí být nejméně jednou ročně přezkoumána generálním ředitelem, aby bylo zajištěno, že zohledňuje:

9.1.1.1. aktualizace příslušných právních předpisů (např. GDPR, DORA),

9.1.1.2. nové podnikové systémy nebo výměnu dat s třetími stranami,

9.1.1.3. zpětnou vazbu z auditů nebo incidentů souvisejících s použitím nemaskovaných dat.

9.2. Mimořádné přezkumy

9.2.1. Přezkumy musí proběhnout také tehdy, když:

9.2.1.1. jsou zavedeny nové aplikace nebo platformy zpracovávající citlivá data,

9.2.1.2. závažný incident odhalí nedostatky ve stávajících opatřeních transformace,

9.2.1.3. změny úrovní klasifikace ovlivní postupy nakládání s daty.

9.3. Řízení verzí a řízení změn

9.3.1. Všechny změny politiky musí být:

9.3.1.1. schváleny GM a zdokumentovány v přehledu změn,

9.3.1.2. jasně komunikovány dotčeným zaměstnancům a poskytovatelům služeb,

9.3.1.3. bezpečně archivovány s omezeným přístupem k neaktuálním verzím.

10. Související politiky a vazby

10.1. Tato politika musí být uplatňována společně s následujícími politikami SME, aby byla zajištěna konzistentní a vymahatelná ochrana citlivých dat:

10.1.1. P13S – Politika klasifikace dat a označování: Definuje úrovně klasifikace (např. „Důvěrné – osobní“), které určují, kdy musí být použito maskování nebo pseudonymizace. Tato politika vynucuje pravidla transformace podle úrovně citlivosti dat.

10.1.2. P14S – Politika uchovávání a likvidace dat: Zajišťuje, aby transformované datové sady, včetně záloh obsahujících maskovaná nebo pseudonymizovaná data, byly uchovávány a likvidovány podle příslušných pravidel, včetně mazání mapovacích klíčů, jakmile již nejsou potřebné.

10.1.3. P17S – Politika ochrany dat a soukromí: Uvádí postupy transformace do souladu s širšími povinnostmi v oblasti soukromí, včetně požadavků GDPR na minimalizaci údajů a používání pseudonymizace jako ochranného opatření při zpracování osobních údajů.

10.1.4. P30S – Politika reakce na incidenty: Upravuje postupy hlášení a eskalace v případě neoprávněného zpřístupnění dat, včetně nesprávného použití nebo zpětného převodu maskovaných či pseudonymizovaných dat.

10.1.5. P2S – Politika rolí a odpovědností v oblasti správy a řízení: Stanoví celkovou odpovědnost za implementaci politiky, akceptaci rizika a schvalování výjimek, zejména na straně generálního ředitele.

10.2. Tyto politiky tvoří integrovaný rámec ochrany dat a zajišťují, že činnosti maskování a pseudonymizace podporují certifikaci ISO 27001 i soulad napříč regulačními požadavky.

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Článek 6.1.3: Vyžaduje ošetření rizik bezpečnosti informací, včetně zmírnění expozice prostřednictvím technik transformace dat.

11.1.2. Článek 8.1: Ukládá implementaci opatření nezbytných ke splnění bezpečnostních cílů, včetně pseudonymizace a maskování.

11.2. ISO/IEC 27002

11.2.1. Opatření 8.11: Poskytuje pokyny k maskování citlivých dat v testovacích a vývojových systémech.

11.2.2. Opatření 8.12: Nabízí postupy prevence úniku dat prostřednictvím řízené transformace a postupů přístupu.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Zajišťuje důvěrnost informací prostřednictvím zastření dat.

11.3.2. SC-28: Chrání informace v klidu i při používání.

11.3.3. PT-2/PT-3: Podporují používání technologií zvyšujících ochranu soukromí, včetně pseudonymizace, při zpracování osobně identifikovatelných údajů.

11.4. GDPR

11.4.1. Článek 4(5): Právně vymezuje pseudonymizaci a ukládá opatření nad mapovacími klíči a identifikátory.

11.4.2. Článek 5(1)(c): Podporuje zásady minimalizace údajů prostřednictvím maskování.

11.4.3. Článek 32: Uznává pseudonymizaci jako technické opatření snižující rizika pro soukromí.

11.5. směrnice NIS2

11.5.1. Článek 21(2)(c): Vyžaduje přiměřená technická opatření k minimalizaci rizik bezpečnosti dat, včetně pseudonymizace jako součásti řízení rizik.

11.6. nařízení DORA

11.6.1. Článek 10(1): Vyžaduje opatření pro řízení rizik souvisejících s ICT, která zahrnují ochranná opatření transformace dat pro zachování kontinuity a důvěrnosti při outsourcingu a vývoji systémů.

11.7. COBIT 2019

11.7.1. DSS05.01: Vyžaduje ochranu informačních aktiv, včetně transformace tam, kde je to možné.

11.7.2. DSS06.06: Požaduje vhodné techniky zastření a pseudonymizace za účelem omezení expozice dat v prostředích s nižší úrovní důvěry.