					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P16S					Naslov dokumenta: **Politika maskiranja podatkov in psevdonimizacije**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 6.1.3, klavzula 8	Tveganja informacijske varnosti in potrebne kontrole, vključno z maskiranjem in psevdonimizacijo
ISO/IEC 27002:2022	Kontroli 8.11, 8.12	Usmeritve za maskiranje in preprečevanje uhajanja podatkov
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Prikrivanje podatkov, tehnologije za izboljšanje zasebnosti
EU NIS2	Člen 21(2)(c)	Sorazmerni tehnični ukrepi, psevdonimizacija kot kontrola
EU DORA	Člen 10(1)	Kontrole tveganj IKT, vključno z zaščitnimi ukrepi pri transformaciji podatkov
COBIT 2019	DSS05.01, DSS06	Varstvo podatkov, tehnike prikrivanja in psevdonimizacije
EU GDPR	Členi 4(5), 5(1)(c), 32	Minimizacija podatkov, psevdonimizacija kot tehnična kontrola

1. Namen

1.1. Ta politika določa zavezujoče zahteve za uporabo maskiranja podatkov in psevdonimizacije za zaščito občutljivih, osebnih in zaupnih podatkov v malih in srednje velikih podjetjih (MSP).

1.2. Ti tehniki sta obvezni, kadar uporaba dejanskih podatkov ni potrebna, na primer pri razvoju, analitiki ali sodelovanju s ponudniki storitev tretjih oseb, saj zmanjšujeta tveganje razkritja, neustrezne uporabe ali kršitev.

1.3. Ta politika neposredno podpira skladnost s standardom ISO/IEC 27001:2022 ter evropskimi regulativnimi zahtevami, kot so Uredba GDPR, Direktiva NIS2 in Uredba DORA.

1.4. S transformacijo podatkov pred njihovo uporabo zunaj prvotnega poslovnega konteksta organizacija omejuje odgovornost in krepi zmožnost dokazovanja potrebne skrbnosti na področju zasebnosti in varnosti.

2. Področje uporabe

2.1. Ta politika se uporablja za vse strukturirane ali nestrukturirane podatke, razvrščene kot osebni, zaupni ali občutljivi, ne glede na to, ali se hranijo ali obdelujejo:

2.1.1. v produkcijskih, testnih ali razvojnih okoljih,

2.1.2. na lokalnih napravah, strežnikih ali platformah v oblaku,

2.1.3. s strani notranjega osebja, pogodbenih izvajalcev ali ponudnikov tretjih oseb.

2.2. Zajema tudi vsa orodja za transformacijo podatkov (maskiranje, tokenizacija, psevdonimizacija), ne glede na to, ali so odprtokodna, komercialna ali razvita znotraj organizacije.

2.3. Primeri uporabe v okviru te politike vključujejo:

2.3.1. pripravo testnih ali razvojnih naborov podatkov,

2.3.2. izvoz podatkov v analitične sisteme,

2.3.3. dostop dobaviteljev ali svetovalcev do operativnih sistemov,

2.3.4. minimizacijo osebnih podatkov za zmanjšanje tveganja obdelave.

3. Cilji

3.1. Zagotoviti, da dejanski osebni ali občutljivi podatki nikoli niso izpostavljeni v okoljih z nižjo ravnjo varnosti, kjer niso nujno potrebni.

3.2. Zahtevati uporabo maskiranja ali psevdonimizacije, kadar dejanski identifikatorji za izvedbo naloge niso strogo potrebni.

3.3. Preprečiti nepooblaščen dostop ali neustrezno uporabo podatkov z uvedbo kontrol transformacije pred prenosom ali obdelavo podatkov.

3.4. Zagotoviti, da so vsi postopki maskiranja in psevdonimizacije sledljivi, revizijsko ustrezni in izvedeni z odobrenimi orodji.

3.5. Zagotoviti skladnost z veljavnimi pravnimi in regulativnimi zahtevami, ki zahtevajo minimizacijo podatkov, zaupnost in zaščitne ukrepe pri transformaciji.

4. Vloge in odgovornosti

4.1. glavni direktor (GM)

4.1.1. je lastnik te politike in jo odobri,

4.1.2. zagotovi, da vsi oddelki in ponudniki izpolnjujejo zahteve glede transformacije podatkov,

4.1.3. pregleduje izjeme, ocene tveganj in dnevnike transformacij,

4.1.4. usklajuje pravne, operativne in dobaviteljske ukrepe v primeru kršitev.

4.2. ponudnik podpore IT / notranja služba IT

4.2.1. izbere in upravlja orodja za maskiranje ali psevdonimizacijo,

4.2.2. zagotovi uporabo ustreznih metod transformacije glede na vrsto podatkov,

4.2.3. vodi dnevnike transformiranih naborov podatkov in postopkov upravljanja ključev,

4.2.4. zagotovi, da se maskiranje izvede pred uporabo za testiranje, s strani dobaviteljev ali za analitiko.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1. Letni pregled

9.1.1. To politiko mora glavni direktor pregledati najmanj enkrat letno, da zagotovi, da odraža:

9.1.1.1. posodobitve veljavnih predpisov (npr. GDPR, DORA),

9.1.1.2. nove poslovne sisteme ali izmenjave podatkov s tretjimi osebami,

9.1.1.3. povratne informacije iz presoj ali incidentov, povezanih z uporabo nemaskiranih podatkov.

9.2. Vmesni pregledi

9.2.1. Pregledi se morajo izvesti tudi, kadar:

9.2.1.1. se uvedejo nove aplikacije ali platforme, ki obdelujejo občutljive podatke,

9.2.1.2. večji incident razkrije vrzeli v obstoječih kontrolah transformacije,

9.2.1.3. spremembe ravni razvrščanja vplivajo na postopke ravnanja s podatki.

9.3. Nadzor različic in upravljanje sprememb

9.3.1. Vse spremembe politike morajo biti:

9.3.1.1. odobrene s strani glavnega direktorja in dokumentirane v evidenci sprememb,

9.3.1.2. jasno sporočene zadevnim zaposlenim in ponudnikom storitev,

9.3.1.3. varno arhivirane z omejenim dostopom do zastarelih različic.

10. Povezane politike in povezave

10.1. Ta politika se mora uporabljati skupaj z naslednjimi politikami SME, da se zagotovi dosledno in izvršljivo varstvo občutljivih podatkov:

10.1.1. P13S – Politika razvrščanja in označevanja podatkov: določa ravni razvrščanja (npr. »zaupno – osebni podatki«), ki določajo, kdaj je treba uporabiti maskiranje ali psevdonimizacijo. Ta politika uveljavlja pravila transformacije glede na ravni občutljivosti podatkov.

10.1.2. P14S – Politika hrambe in odstranjevanja podatkov: zagotavlja, da se transformirani nabori podatkov, vključno z varnostnimi kopijami, ki vsebujejo maskirane ali psevdonimizirane podatke, hranijo in odstranjujejo v skladu z veljavnimi pravili, vključno z izbrisom ključev za preslikavo, ko ti niso več potrebni.

10.1.3. P17S – Politika varstva podatkov in zasebnosti: usklajuje prakse transformacije s širšimi obveznostmi glede zasebnosti, vključno z zahtevami GDPR za minimizacijo podatkov in uporabo psevdonimizacije kot varovalnega ukrepa pri obdelavi osebnih podatkov.

10.1.4. P30S – Politika odzivanja na incidente: zajema postopke poročanja in eskalacije v primeru nepooblaščenega razkritja podatkov, vključno z neustrezno uporabo ali povrnitvijo maskiranih ali psevdonimiziranih podatkov.

10.1.5. P2S – Politika vlog in odgovornosti upravljanja: določa celovito odgovornost za izvajanje politike, sprejemanje tveganj in odobritev izjem, predvsem glavnemu direktorju.

10.2. Te politike tvorijo integriran okvir varstva podatkov, ki zagotavlja, da dejavnosti maskiranja in psevdonimizacije podpirajo skladnost z ISO 27001 in medregulativno skladnost.

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001

11.1.1. Klavzula 6.1.3: zahteva obravnavo tveganj informacijske varnosti, kar vključuje zmanjševanje izpostavljenosti s tehnikami transformacije podatkov.

11.1.2. Klavzula 8.1: zahteva uvedbo kontrol, potrebnih za doseganje varnostnih ciljev, vključno s psevdonimizacijo in maskiranjem.

11.2. ISO/IEC 27002

11.2.1. Kontrola 8.11: podaja usmeritve za maskiranje občutljivih podatkov v testnih in razvojnih sistemih.

11.2.2. Kontrola 8.12: določa pristope za preprečevanje uhajanja podatkov z nadzorovano transformacijo in praksami dostopa.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: zagotavlja zaupnost informacij s prikrivanjem podatkov.

11.3.2. SC-28: varuje informacije v mirovanju in med uporabo.

11.3.3. PT-2/PT-3: spodbujata uporabo tehnologij za izboljšanje zasebnosti, vključno s psevdonimizacijo, pri obdelavi osebnih podatkov.

11.4. EU GDPR

11.4.1. Člen 4(5): pravno opredeljuje psevdonimizacijo in zahteva kontrole nad ključi za preslikavo in identifikatorji.

11.4.2. Člen 5(1)(c): podpira načelo minimizacije podatkov z maskiranjem.

11.4.3. Člen 32: priznava psevdonimizacijo kot tehnično kontrolo, ki zmanjšuje tveganja za zasebnost.

11.5. Direktiva EU NIS2

11.5.1. Člen 21(2)(c): zahteva sorazmerne tehnične ukrepe za zmanjšanje tveganja glede varnosti podatkov, vključno s psevdonimizacijo kot delom obvladovanja tveganj.

11.6. Uredba EU DORA

11.6.1. Člen 10(1): zahteva kontrole tveganj, povezanih z IKT, ki vključujejo zaščitne ukrepe pri transformaciji podatkov za neprekinjeno poslovanje in zaupnost med zunanjim izvajanjem in razvojem sistemov.

11.7. COBIT 2019

11.7.1. DSS05.01: zahteva zaščito informacijskih sredstev, vključno s transformacijo, kjer je to mogoče.

11.7.2. DSS06.06: zahteva ustrezne tehnike prikrivanja in psevdonimizacije za omejitev izpostavljenosti podatkov v okoljih z nižjo ravnjo zaupanja.