					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P16					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	Splošne zahteve za obravnavo tveganj in operativne kontrole za maskiranje in psevdonimizacijo
ISO/IEC 27002:2022	Kontroli 8.11, 8	Smernice za izvajanje maskiranja in psevdonimizacije
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Kontrole zasebnosti in zaupnosti za minimizacijo podatkov, preoblikovanje podatkov in omejevanje dostopa
Uredba EU GDPR	Členi 4(5), 5(1)(c,f), 32	Pravna podlaga in zahteve za psevdonimizacijo ter ukrepe varstva podatkov
Direktiva EU NIS2	Člen 21(2)(c)	Obveznost tehničnih in organizacijskih ukrepov, vključno s tehnologijami za izboljšanje zasebnosti (PET)
Uredba EU DORA	Člena 10(1), 10(2)(e)	Upravljanje tveganj IKT in kontrole zaupnosti za maskiranje podatkov in psevdonimizacijo
COBIT 2019	DSS05.01, DSS06.06, MEA03	Kontrole upravljanja za varstvo podatkov z uporabo maskiranja ter presojo skladnosti

1. Namen

1.1 Ta politika določa pristop organizacije k izvajanju maskiranja podatkov in psevdonimizacije kot tehnologij za izboljšanje zasebnosti (PET) za zmanjšanje možnosti identifikacije ter izpostavljenosti osebnih ali občutljivih podatkov.

1.2 Podpira varno uporabo informacij pri testiranju, analitiki in operativnem delu ter hkrati zagotavlja skladnost s pravnimi in regulativnimi zahtevami, zmanjšuje vpliv kršitev in uveljavlja načeli minimizacije podatkov in zaupnosti.

1.3 Politika je usklajena z ISO/IEC 27001:2022, podpira člen 4(5) GDPR glede psevdonimizacije ter vključuje na tveganjih temelječe izvajanje v skladu s standardi NIST, NIS2, DORA in COBIT 2019.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse zaposlene, pogodbene izvajalce, tretje osebe ali dobavitelje, ki imajo dostop do sistemov, v katerih se obdelujejo osebni, zaupni ali občutljivi podatki;

2.1.2 vsa podatkovna okolja, vključno s produkcijskim, razvojnim, testnim in pripravljalnim okoljem;

2.1.3 vse oblike maskiranja podatkov (npr. statično, dinamično, deterministično, tokenizacija) in tehnike psevdonimizacije, ki se uporabljajo za zmanjševanje tveganj za zasebnost;

2.1.4 vse vrste podatkov (strukturirani ali nestrukturirani podatki), sisteme (v lastnih prostorih ali gostovane v oblaku) in aplikacije, ki vključujejo osebne ali regulirane podatke.

2.2 Področje uporabe vključuje uporabo pri:

2.2.1 razvoju aplikacij ter v okoljih za zagotavljanje kakovosti (QA) in testiranje;

2.2.2 analitičnih platformah ali platformah za poročanje;

2.2.3 izmenjavi podatkov s tretjimi osebami ali ponudniki storitev;

2.2.4 sistemih za varnostno kopiranje, arhiviranje ali obnovo.

3. Cilji

3.1 Zagotoviti dosledno in učinkovito uporabo maskiranja in psevdonimizacije za zmanjšanje tveganj izpostavljenosti podatkov ali neustrezne uporabe.

3.2 Zagotoviti, da se resnični podatki nikoli ne uporabljajo v neprodukcijskih okoljih, razen če so bili preoblikovani z odobrenimi tehnikami PET.

3.3 Kadar je to potrebno zaradi operativne doslednosti, ohraniti referenčno integriteto, uporabnost in preoblikovanja, ki ohranjajo obliko.

3.4 Uveljaviti stroge kontrole dostopa do izvornih podatkov, maskiranih podatkov in ključev za ponovno identifikacijo.

3.5 Maskirane ali psevdonimizirane podatkovne nize obravnavati kot občutljive podatke, za katere veljajo revizijske sledi, kontrole hrambe in postopki odzivanja na incidente.

3.6 Učinkovitost teh kontrol potrjevati z neprekinjenim testiranjem, spremljanjem in revizijskimi postopki.

4. Vloge in odgovornosti

4.1 Najvišje vodstvo

4.1.1 Odobri to politiko in zagotovi njeno izvajanje kot del širših pobud upravljanja IT in varstva podatkov.

4.2 Vodja informacijske varnosti (CISO) / vodja ISMS

4.2.1 Nadzira izvajanje in stalno skladnost.

4.2.2 Zagotavlja usklajenost s klavzulo 6.1.3 standarda ISO/IEC 27001 (obravnava tveganj) in klavzulo 8.1 (operativno upravljanje).

4.2.3 Pregleduje revizijske dnevnike in potrjuje učinkovitost kontrol.

[... 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 To politiko je treba pregledati najmanj enkrat letno ali prej v primeru:

9.1.1 regulativnih sprememb, ki vplivajo na maskiranje ali psevdonimizacijo;

9.1.2 uvedbe novih sistemov IT, ki obdelujejo občutljive podatke;

9.1.3 bistvenih sprememb sheme razvrščanja podatkov v organizaciji;

9.1.4 ugotovitev presoje, ki kažejo na pomanjkljivosti kontrol;

9.1.5 pojava novih groženj ali tehnologij maskiranja.

9.2 Vodja ISMS vodi pregled v sodelovanju z DPO, lastniki podatkov, informacijsko varnostjo in pravno službo. Posodobitve morajo biti verzionirane, odobrene s strani izvršnega vodstva in sporočene vsem relevantnim zainteresiranim stranem.

10. Povezane politike in povezave

10.1 P13 - Politika razvrščanja in označevanja podatkov. Odločitve o maskiranju in psevdonimizaciji so neposredno odvisne od razvrstitve podatkovnih polj in ravni občutljivosti, opredeljenih v P13.

10.2 P14 - Politika hrambe podatkov. Preoblikovani podatkovni nizi morajo biti hranjeni in uničeni v skladu s pravili življenjskega cikla iz P14, pri čemer se zagotovi, da se maskirani in psevdonimizirani podatki obravnavajo kot občutljivi.

10.3 P17 - Politika varstva podatkov in zasebnosti. Določa načela zasebnosti in regulativne podlage za uporabo psevdonimizacije kot skladne dejavnosti obdelave po GDPR in podobnih predpisih.

10.4 P22 - Politika beleženja in spremljanja. Omogoča centralizirano revidiranje in opozarjanje glede dogodkov maskiranja in psevdonimizacije v skladu s strukturiranimi protokoli varnostnega spremljanja.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 6.1.3 - načrt obravnave tveganj: določa maskiranje in psevdonimizacijo kot mehanizma obravnave tveganj za zmanjšanje možnosti identifikacije občutljivih podatkov v okoljih obdelave, ki niso nujna za poslovanje.

11.1.2 Klavzula 8.1 - operativno načrtovanje in kontrola: zahteva tehnične in postopkovne kontrole za varno preoblikovanje podatkov med obdelavo, hrambo ali prenosom.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroli 8.11, 8: smernice za maskiranje podatkov in psevdonimizacijo za zmanjšanje tveganj ponovne identifikacije in uhajanja podatkov.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - zaščita PII: izvajanje tehnologij za izboljšanje zasebnosti, kot sta maskiranje in psevdonimizacija.

11.3.2 PT-2, PT-3: minimizacija in varnost obdelave PII - preoblikovanje za zmanjšanje možnosti identifikacije in uveljavljanje nadzora dostopa.

11.3.3 SC-12, SC-28, SC-30: zaupnost in celovitost podatkov - kontrole zaupnosti in prikrivanja za hrambo, prenos in uporabo.

11.4 Uredba EU GDPR (2016/679)

11.4.1 Člen 4(5): formalna opredelitev psevdonimizacije.

11.4.2 Člen 32: varnost obdelave - organizacijski in tehnični ukrepi za psevdonimizacijo.

11.4.3 Člen 5(1)(c,f): minimizacija podatkov in zaupnost z uporabo psevdonimizacije in maskiranja.

11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Člen 21(2)(c): zahteva tehnologije za izboljšanje zasebnosti, kot sta maskiranje in psevdonimizacija, kot varnostne ukrepe.

11.6 Uredba EU DORA (2022/2554)

11.6.1 Člen 10(1): okvir upravljanja IKT-tveganj vključuje kontrole maskiranja in psevdonimizacije.

11.6.2 Člen 10(2)(e): zahteva uporabo tehnologij preoblikovanja za zaščito osebnih in finančnih podatkov.

11.7 COBIT 2019

11.7.1 DSS05.01: zaščita informacijskih sredstev - zahteve za maskiranje in psevdonimizacijo.

11.7.2 DSS06.06: varno testiranje in analitika - maskiranje v okoljih zunaj produkcije.

11.7.3 MEA03: spremljanje skladnosti glede učinkovitosti maskiranja in psevdonimizacije.