					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P16S					Naziv dokumenta: **Politika maskiranja podataka i pseudonimizacije**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 6.1.3, Točka 8	Rizici informacijske sigurnosti i potrebne kontrole, uključujući maskiranje i pseudonimizaciju
ISO/IEC 27002:2022	Kontrole 8.11, 8.12	Smjernice za maskiranje i sprječavanje curenja podataka
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Zamagljivanje podataka i tehnologije za unaprjeđenje privatnosti
EU NIS2	Članak 21(2)(c)	Proporcionalne tehničke mjere, uključujući pseudonimizaciju kao kontrolu
EU DORA	Članak 10(1)	Kontrole IKT rizika, uključujući zaštitne mjere transformacije podataka
COBIT 2019	DSS05.01, DSS06	Zaštita podataka, tehnike zamagljivanja i pseudonimizacije
EU GDPR	Članci 4(5), 5(1)(c), 32	Minimizacija podataka, pseudonimizacija kao tehnička kontrola

1. Svrha

1.1. Ova politika utvrđuje obvezujuće zahtjeve za primjenu maskiranja podataka i pseudonimizacije radi zaštite osjetljivih, osobnih i povjerljivih podataka u malim i srednjim poduzećima (SME).

1.2. Ove tehnike obvezne su kada stvarni podaci nisu nužni, primjerice u razvoju, analitici ili scenarijima pružanja usluga od strane trećih strana, kako bi se smanjio rizik od izlaganja, zlouporabe ili povrede podataka.

1.3. Ova politika izravno podupire usklađenost sa zahtjevima za certifikaciju prema ISO/IEC 27001:2022, kao i s europskim regulatornim zahtjevima kao što su GDPR, Direktiva NIS2 i Uredba DORA.

1.4. Transformacijom podataka prije njihove uporabe izvan izvornog poslovnog konteksta organizacija ograničava izloženost odgovornosti i jača mogućnost dokazivanja dužne pažnje u području privatnosti i sigurnosti.

2. Opseg

2.1. Ova politika primjenjuje se na sve strukturirane i nestrukturirane podatke klasificirane kao osobni, povjerljivi ili osjetljivi, neovisno o tome pohranjuju li se ili obrađuju:

2.1.1. u produkcijskim, testnim ili razvojnim okruženjima

2.1.2. na lokalnim uređajima, poslužiteljima ili platformama u oblaku

2.1.3. od strane internog osoblja, ugovornih izvođača ili pružatelja usluga trećih strana

2.2. Politika obuhvaća i sve alate za transformaciju podataka (maskiranje, tokenizacija, pseudonimizacija), neovisno o tome jesu li otvorenog koda, komercijalni ili razvijeni unutar organizacije.

2.3. Primjeri primjene ove politike uključuju:

2.3.1. pripremu testnih ili razvojnih skupova podataka

2.3.2. izvoz podataka u analitičke sustave

2.3.3. pristup dobavljača ili konzultanata operativnim sustavima

2.3.4. minimizaciju podataka ispitanika radi smanjenja rizika obrade

3. Ciljevi

3.1. Osigurati da stvarni osobni ili osjetljivi podaci nikada ne budu izloženi u okruženjima niže razine sigurnosti kada to nije nužno.

3.2. Propisati primjenu maskiranja ili pseudonimizacije kada stvarni identifikatori nisu strogo potrebni za izvršavanje zadatka.

3.3. Spriječiti neovlašteni pristup ili zlouporabu podataka provedbom kontrola transformacije prije prijenosa ili obrade podataka.

3.4. Osigurati da svi postupci maskiranja i pseudonimizacije budu sljedivi, podložni reviziji i provedeni putem odobrenih alata.

3.5. Ispuniti primjenjive pravne i regulatorne zahtjeve koji nalažu minimizaciju podataka, povjerljivost i zaštitne mjere transformacije.

4. Uloge i odgovornosti

4.1. glavni direktor (GM)

4.1.1. vlasnik je ove politike i odobrava je

4.1.2. osigurava da svi odjeli i pružatelji usluga poštuju zahtjeve transformacije podataka

4.1.3. pregledava iznimke, procjene rizika i evidencije transformacije

4.1.4. koordinira pravne, operativne ili dobavljačke mjere u slučaju kršenja

4.2. pružatelj IT podrške / interni IT

4.2.1. odabire i upravlja alatima za maskiranje ili pseudonimizaciju

4.2.2. osigurava primjenu odgovarajućih metoda transformacije ovisno o vrsti podataka

4.2.3. vodi evidenciju o transformiranim skupovima podataka i postupcima upravljanja ključevima

4.2.4. osigurava da se maskiranje provede prije uporabe u testiranju, od strane dobavljača ili u analitici

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1. Godišnji pregled

9.1.1. Ovu politiku glavni direktor mora pregledati najmanje jednom godišnje kako bi se osiguralo da odražava:

9.1.1.1. ažuriranja primjenjivih propisa (npr. GDPR, DORA)

9.1.1.2. nove poslovne sustave ili razmjenu podataka s trećim stranama

9.1.1.3. povratne informacije iz revizija ili incidenata povezanih s uporabom nemaskiranih podataka

9.2. Izvanredni pregledi

9.2.1. Pregledi se moraju provoditi i kada:

9.2.1.1. se uvode nove aplikacije ili platforme koje obrađuju osjetljive podatke

9.2.1.2. veliki incident otkrije nedostatke u postojećim kontrolama transformacije

9.2.1.3. promjene razina klasifikacije utječu na postupke rukovanja podacima

9.3. upravljanje verzijama i promjenama

9.3.1. Sve promjene politike moraju biti:

9.3.1.1. odobrene od strane GM-a i dokumentirane u zapisniku promjena

9.3.1.2. jasno priopćene zaposlenicima i pružateljima usluga na koje se odnose

9.3.1.3. sigurno arhivirane uz ograničen pristup zastarjelim verzijama

10. Povezane politike i poveznice

10.1. Ova politika mora se primjenjivati zajedno sa sljedećim SME politikama kako bi se osigurala dosljedna i obvezujuća zaštita osjetljivih podataka:

10.1.1. P13S – Politika klasifikacije i označavanja podataka: definira razine klasifikacije (npr. „Povjerljivo – osobni podaci") koje određuju kada se moraju primijeniti maskiranje ili pseudonimizacija. Ova politika provodi pravila transformacije na temelju razine osjetljivosti podataka.

10.1.2. P14S – Politika zadržavanja i zbrinjavanja podataka: osigurava da se transformirani skupovi podataka, uključujući sigurnosne kopije koje sadrže maskirane ili pseudonimizirane podatke, zadržavaju i zbrinjavaju u skladu s primjenjivim pravilima, uključujući brisanje ključeva mapiranja kada više nisu potrebni.

10.1.3. P17S – Politika zaštite podataka i privatnosti: usklađuje prakse transformacije sa širim obvezama privatnosti, uključujući zahtjeve GDPR-a za minimizaciju podataka i uporabu pseudonimizacije kao zaštitne mjere pri obradi osobnih podataka.

10.1.4. P30S – Politika odgovora na incidente: obuhvaća postupke prijavljivanja i eskalacije u slučaju neovlaštenog otkrivanja podataka, uključujući neispravnu uporabu ili povrat maskiranih ili pseudonimiziranih podataka u izvorni oblik.

10.1.5. P2S – Politika uloga i odgovornosti u upravljanju: dodjeljuje ukupnu odgovornost za provedbu politike, prihvaćanje rizika i odobravanje iznimki, prvenstveno glavnom direktoru.

10.2. Ove politike čine integrirani okvir zaštite podataka te osiguravaju da aktivnosti maskiranja i pseudonimizacije podupiru certifikaciju prema ISO 27001 i usklađenost u više regulatornih okvira.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 6.1.3: zahtijeva obradu rizika informacijske sigurnosti, što uključuje ublažavanje izloženosti primjenom tehnika transformacije podataka.

11.1.2. Točka 8.1: nalaže provedbu kontrola potrebnih za ispunjenje sigurnosnih ciljeva, uključujući pseudonimizaciju i maskiranje.

11.2. ISO/IEC 27002

11.2.1. Kontrola 8.11: pruža smjernice za maskiranje osjetljivih podataka u testnim i razvojnim sustavima.

11.2.2. Kontrola 8.12: daje smjernice za sprječavanje curenja podataka putem kontrolirane transformacije i kontrola pristupa.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: osigurava povjerljivost informacija zamagljivanjem podataka.

11.3.2. SC-28: štiti podatke u mirovanju i tijekom uporabe.

11.3.3. PT-2/PT-3: promiču uporabu tehnologija za unaprjeđenje privatnosti, uključujući pseudonimizaciju, pri obradi osobnih podataka.

11.4. EU GDPR

11.4.1. Članak 4(5): pravno definira pseudonimizaciju i nalaže kontrole nad ključevima mapiranja i identifikatorima.

11.4.2. Članak 5(1)(c): podupire načelo minimizacije podataka primjenom maskiranja.

11.4.3. Članak 32: prepoznaje pseudonimizaciju kao tehničku kontrolu koja smanjuje rizike za privatnost.

11.5. Direktiva EU NIS2

11.5.1. Članak 21(2)(c): zahtijeva proporcionalne tehničke mjere radi smanjenja rizika za sigurnost podataka, uključujući pseudonimizaciju kao dio kontrola rizika.

11.6. Uredba EU DORA

11.6.1. Članak 10(1): nalaže kontrole rizika povezanih s IKT-om koje uključuju zaštitne mjere transformacije podataka radi kontinuiteta i povjerljivosti tijekom izdvajanja usluga i razvoja sustava.

11.7. COBIT 2019

11.7.1. DSS05.01: zahtijeva zaštitu informacijske imovine, uključujući transformaciju gdje je to primjenjivo.

11.7.2. DSS06.06: zahtijeva odgovarajuće tehnike zamagljivanja i pseudonimizacije radi ograničavanja izloženosti podataka u okruženjima niže razine povjerenja.