| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ovdje unesite naziv registrirane pravne osobe | | | | | | | |
| Broj dokumenta:<br>P16 | | | | | Naziv dokumenta:<br>**Politika maskiranja podataka i pseudonimizacije** | | | | | | | |
| Verzija:<br>1.0 | | Datum stupanja na snagu:<br>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** |
| | | | |
| | | | |

Usklađenost sa standardima i propisima

| Standard/regulativa | Točka/članak | Napomena |
|---|---|---|
| ISO/IEC 27001:2022 | Točka 6.1 | Opći zahtjevi za upravljanje rizicima i operativne kontrole za maskiranje i pseudonimizaciju |
| ISO/IEC 27002:2022 | Kontrole 8.11, 8 | Smjernice za provedbu maskiranja i pseudonimizacije |
| GDPR EU | Članci 4(5), 5(1)(c,f), 32 | Pravna osnova i zahtjevi za pseudonimizaciju te mjere zaštite podataka |
| Direktiva EU NIS2 | Članak 21(2)(c) | Obveza primjene tehničkih i organizacijskih mjera, uključujući tehnologije za unapređenje privatnosti (PET) |
| Uredba EU DORA | Članci 10(1), 10(2)(e) | Upravljanje IKT rizicima i kontrole povjerljivosti za maskiranje podataka i pseudonimizaciju |
| COBIT 2019 | DSS05.01, DSS06.06, MEA | Upravljačke kontrole za zaštitu podataka primjenom maskiranja i procjenom usklađenosti |

**1. Svrha**

1.1 Ova politika definira pristup organizacije provedbi maskiranja podataka i pseudonimizacije kao tehnologija za unapređenje privatnosti (PET) radi smanjenja mogućnosti identifikacije te izloženosti osobnih ili osjetljivih podataka.

1.2 Ova politika podupire sigurnu uporabu informacija u testiranju, analitici i operativnim aktivnostima, uz istodobno osiguravanje usklađenosti sa zakonskim i regulatornim zahtjevima, ublažavanje učinka povreda te primjenu načela minimizacije podataka i povjerljivosti.

1.3 Ova je politika usklađena s normom ISO/IEC 27001:2022, podupire članak 4(5) GDPR-a EU u dijelu koji se odnosi na pseudonimizaciju te uključuje provedbu utemeljenu na riziku u skladu sa standardima NIST, NIS2, DORA i COBIT 2019.

**2. Područje primjene**

**2.1 Ova politika primjenjuje se na:**

2.1.1 sve zaposlenike, ugovorne izvođače, treće strane i dobavljače koji imaju pristup sustavima koji obrađuju osobne, povjerljive ili osjetljive informacije.

2.1.2 sva podatkovna okruženja, uključujući produkcijska, razvojna, testna i pripremna okruženja.

2.1.3 sve oblike maskiranja podataka (npr. statičko, dinamičko, deterministično, tokenizacija) i tehnike pseudonimizacije koje se koriste za smanjenje rizika za privatnost.

2.1.4 sve vrste podataka (strukturirane ili nestrukturirane), sustave (lokalne ili hostirane u oblaku) i aplikacije koje uključuju osobne ili regulirane podatke.

**2.2 Područje primjene uključuje uporabu u:**

2.2.1 razvoju aplikacija te QA i testnim okruženjima

2.2.2 analitičkim platformama ili platformama za izvješćivanje

2.2.3 razmjeni podataka s trećim stranama ili pružateljima usluga

2.2.4 sustavima za sigurnosne kopije, arhiviranje ili oporavak

**3. Ciljevi**

3.1 Osigurati dosljednu i djelotvornu primjenu maskiranja i pseudonimizacije radi smanjenja rizika od izloženosti podataka ili njihove zlouporabe.

3.2 Osigurati da se stvarni podaci nikada ne koriste u neprodukcijskim okruženjima, osim ako su prethodno transformirani primjenom odobrenih PET tehnika.

3.3 Održavati referencijalnu cjelovitost, uporabljivost i transformacije koje čuvaju format kada je to potrebno radi operativne dosljednosti.

3.4 Provoditi strogu kontrolu pristupa izvornim podacima, maskiranim podacima i ključevima za ponovnu identifikaciju.

3.5 Maskirane ili pseudonimizirane skupove podataka tretirati kao osjetljive podatke, uz primjenu revizijskog bilježenja pristupa, kontrola zadržavanja i protokola odgovora na incidente.

3.6 Potvrđivati djelotvornost tih kontrola putem kontinuiranog testiranja, praćenja i revizijskih postupaka.

**4. Uloge i odgovornosti**

**4.1 Izvršno rukovodstvo**

4.1.1 Odobrava ovu politiku i osigurava njezinu provedbu kao dio šireg upravljanja informacijskim tehnologijama i inicijativa zaštite podataka.

**4.2 Glavni službenik za informacijsku sigurnost (CISO) / voditelj ISMS-a**

4.2.1 Nadzire provedbu i trajnu usklađenost.

4.2.2 Osigurava usklađenost s točkom 6.1.3 norme ISO/IEC 27001 (obrada rizika) i točkom 8.1 (operativna kontrola).

4.2.3 Pregledava revizijske zapise i potvrđuje djelotvornost kontrola.

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

**9. Zahtjevi za pregled i ažuriranje**

**9.1 Ova politika mora se pregledati najmanje jednom godišnje ili ranije u slučaju:**

9.1.1 regulatornih promjena koje utječu na maskiranje ili pseudonimizaciju

9.1.2 uvođenja novih IT sustava koji obrađuju osjetljive podatke

9.1.3 značajnih promjena u shemi klasifikacije podataka organizacije

9.1.4 nalaza revizije koji ukazuju na nedostatke kontrola

9.1.5 pojave novih prijetnji ili tehnologija maskiranja

9.2 Voditelj ISMS-a vodi pregled u savjetovanju sa službenikom za zaštitu podataka (DPO), vlasnicima podataka, informacijskom sigurnošću i pravnom službom. Ažuriranja moraju biti pod verzijskom kontrolom, odobrena od strane najvišeg rukovodstva i priopćena svim pogođenim dionicima.

**10. Povezane politike i poveznice**

10.1 P13 - Politika klasifikacije podataka i označavanja. Odluke o maskiranju i pseudonimizaciji izravno ovise o klasifikaciji podatkovnih polja i razinama osjetljivosti definiranima u dokumentu P13.

10.2 P14 - Politika zadržavanja i zbrinjavanja podataka. Transformirani skupovi podataka moraju se zadržavati i zbrinjavati u skladu s pravilima životnog ciklusa iz dokumenta P14, uz osiguravanje da se maskirani i pseudonimizirani podaci tretiraju kao osjetljivi.

10.3 P17 - Politika zaštite podataka i privatnosti. Utvrđuje načela privatnosti i regulatorne osnove za primjenu pseudonimizacije kao usklađene aktivnosti obrade prema GDPR-u i sličnim propisima.

10.4 P22 - Politika revizijskog bilježenja i praćenja. Omogućuje centraliziranu reviziju i upozoravanje na događaje maskiranja i pseudonimizacije u skladu sa strukturiranim protokolima sigurnosnog praćenja.

## 11. Referentni standardi i okviri

### 11.1 ISO/IEC 27001

11.1.1 Točka 6.1.3 - plan obrade rizika: utvrđuje maskiranje i pseudonimizaciju kao mehanizme obrade rizika za smanjenje mogućnosti identifikacije osjetljivih podataka u okruženjima obrade koja nisu nužna za osnovne poslovne potrebe.

11.1.2 Točka 8.1 - operativno planiranje i kontrola: nalaže tehničke i postupovne kontrole za sigurnu transformaciju podataka tijekom obrade, pohrane ili prijenosa.

### 11.2 ISO/IEC 27002:2022

11.2.1 Kontrole 8.11, 8: smjernice za maskiranje podataka i pseudonimizaciju radi smanjenja rizika od ponovne identifikacije i curenja podataka.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - zaštita osobno identifikacijskih podataka: provedba tehnologija za unapređenje privatnosti kao što su maskiranje i pseudonimizacija.

11.3.2 PT-2, PT-3: minimizacija i sigurnost obrade osobno identifikacijskih podataka - transformacija radi smanjenja mogućnosti identifikacije i provedbe kontrole pristupa.

11.3.3 SC-12, SC-28, SC-30: povjerljivost i cjelovitost podataka - kontrole povjerljivosti i prikrivanja za pohranu, prijenos i uporabu.

### 11.4 GDPR EU (2016/679)

11.4.1 Članak 4(5): formalna definicija pseudonimizacije.

11.4.2 Članak 32: sigurnost obrade - organizacijske i tehničke mjere za pseudonimizaciju.

11.4.3 Članak 5(1)(c,f): minimizacija podataka i povjerljivost primjenom pseudonimizacije i maskiranja.

### 11.5 Direktiva EU NIS2 (2022/2555)

11.5.1 Članak 21(2)(c): zahtijeva PET tehnologije poput maskiranja i pseudonimizacije kao sigurnosne mjere.

### 11.6 Uredba EU DORA (2022/2554)

11.6.1 Članak 10(1): okvir za upravljanje IKT rizicima uključuje kontrole maskiranja i pseudonimizacije.

11.6.2 Članak 10(2)(e): nalaže uporabu tehnologija transformacije radi zaštite osobnih i financijskih podataka.

### 11.7 COBIT 2019

11.7.1 DSS05.01: zaštita informacijske imovine - zahtjevi za maskiranje i pseudonimizaciju.

11.7.2 DSS06.06: sigurno testiranje i analitika - maskiranje u okruženjima izvan produkcije.

11.7.3 MEA03: praćenje usklađenosti djelotvornosti maskiranja i pseudonimizacije.