

				Dañhal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P16S				Titlu tad-dokument: Politika dwar il-Masking tad-Data u l-Pseudonimizzazzjoni							
Verżjoni: 1.0		Data tad-dħul fis-seħħ: 01.01.2025		Sid tad-dokument:							
X	Politika		Standard		Proċedura		Formola		Registru		Ohra

Storja tar-reviżjonijiet				
Numru tar-reviżjoni	Data tar-reviżjoni	Bidliet	Ivvedut minn	Sid tal-proċess

Approvazzjonijiet			
Isem	Pożizzjoni	Data	Firma

Avviż legali (drittijiet tal-awtur u restrizzjonijiet fuq l-użu)
(C) 2025 Clarysec LLC. All rights reserved.

Dan id-dokument huwa proprjetà intellettuali ta' Clarysec LLC. L-ebda parti minn dan id-dokument ma tista' tiġi kkupjata, użata mill-ġdid, distribwita jew modifikata għal skopijiet kummerċjali jew ta' implimentazzjoni mingħajr awtorizzazzjoni espliċita minn qabel bil-miktub.

L-użu mhux awtorizzat huwa strettament ipprojbit u jista' jwassal għal azzjoni legali.

Għal-liċenzjar, ikkuntattja: info@clarysec.com

Allinjata ma' standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 6.1.3, Klawżola 8	Riskji għas-sigurtà tal-informazzjoni u l-kontrolli meħtieġa, inkluż il-masking u l-pseudonimizzazzjoni
ISO/IEC 27002:2022	Kontrolli 8.11, 8.12	Gwida dwar il-masking u l-prevenzjoni ta' tnixxija tad-data
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Oskurament tad-data u teknoloġiji li jsaħħu l-privatezza
EU NIS2	Artikolu 21(2)(c)	Miżuri tekniċi proporzjonati, inkluża l-pseudonimizzazzjoni bħala kontroll
EU DORA	Artikolu 10(1)	Kontrolli tar-riskju tal-ICT, inklużi salvagwardji ta' trasformazzjoni
COBIT 2019	DSS05.01, DSS06	Protezzjoni tad-data u tekniki ta' oskurament/pseudonimizzazzjoni
GDPR tal-UE	Artikoli 4(5), 5(1)(c), 32	Minimizzazzjoni tad-data u pseudonimizzazzjoni bħala kontroll tekniku

1. Għan

1.1. Din il-politika tiddefinixxi rekwiżiti vinkolanti għall-użu tal-masking tad-data u tal-pseudonimizzazzjoni sabiex tiġi protetta data sensittiva, personali u kunfidenzjali fi ħdan intrapriži żgħar u ta' daqs medju (SMEs).

1.2. Dawn it-tekniki huma obligatorji meta d-data reali ma tkunx meħtieġa, bħall-iżvilupp, l-analitika jew xenarji ta' servizzi pprovduti minn partijiet terzi, u jgħinu biex jitnaqqsu r-riskji ta' espożizzjoni, użu hażin jew ksur tad-data.

1.3. Din il-politika tappoġġja direttament il-konformità maċ-ċertifikazzjoni ISO/IEC 27001:2022, kif ukoll ma' obbligi regolatorji Ewropej bħall-GDPR, id-Direttiva NIS2 u r-Regolament DORA.

1.4. Permezz tat-trasformazzjoni tad-data qabel l-użu tagħha barra mill-kuntest oriġinali tan-negozju, l-organizzazzjoni tillimita r-responsabbiltà u ssaħħaħ il-kapaċità tagħha li turi konformità u diliġenza dovuta fir-rigward tal-privatezza u s-sigurtà.

2. Kamp ta' applikazzjoni

2.1. Din il-politika tapplika għad-data strutturata u mhux strutturata kollha kklassifikata bħala personali, kunfidenzjali jew sensittiva, kemm jekk maħzuna kif ukoll jekk ipproċessata:

2.1.1. F'ambjenti ta' produzzjoni, test jew żvilupp

2.1.2. Fuq apparati lokali, servers jew pjattaformi cloud

2.1.3. Minn persunal intern, kuntratturi jew fornituri ta' servizzi ta' partijiet terzi

2.2. Tkopri wkoll l-għodod kollha għat-trasformazzjoni tad-data (masking, tokenization, pseudonimizzazzjoni), kemm jekk open-source, kummerċjali jew żviluppanti internament.

2.3. Każijiet ta' użu taħt din il-politika jinkludu:

2.3.1. It-tnejn ta' settijiet tad-data għat-test jew għall-iżvilupp

2.3.2. L-esportazzjoni tad-data lejn sistemi analitiċi

2.3.3. Aċċess minn fornituri jew konsulenti għal sistemi operattivi

2.3.4. Il-minimizzazzjoni tad-data tas-suġġett tad-data sabiex jitnaqqas ir-riskju tal-ipproċessar

3. Obiettivi

3.1. Jiġi żgurat li data personali jew sensitiva reali qatt ma tiġi esposta f'ambjenti b'livell ta' sigurtà aktar baxx fejn ma tkunx essenzjali.

3.2. Jiġi impost l-użu ta' tekniki ta' masking jew psewdonimizzazzjoni meta identifikaturi reali ma jkunux strettament meħtieġa għall-kompitu.

3.3. Jiġi evitat aċċess mhux awtorizzat jew użu ħażin tad-data billi jiġu applikati kontrolli ta' trasformazzjoni qabel it-trasferiment jew l-ipproċessar tad-data.

3.4. Jiġi żgurat li l-proċessi kollha ta' masking u psewdonimizzazzjoni jkollhom traċċabbiltà, ikunu awditabbli u jiġu applikati permezz ta' għodod approvati.

3.5. Tinkiseb konformità ma' standards legali u regolatorji applikabbli li jeħtieġu minimizzazzjoni tad-data, kunfidenzjalità u salvagwardji ta' trasformazzjoni.

4. Rwoli u responsabbiltajiet

4.1. Maniġer Ġenerali (GM)

4.1.1. Huwa s-sid ta' din il-politika u japprova

4.1.2. Jiżgura li d-dipartimenti u l-fornituri kollha jikkonformaw mar-rekwiżiti tat-trasformazzjoni

4.1.3. Jagħmel rieżami tal-eċċezzjonijiet, tal-evalwazzjonijiet tar-riskju u tal-logs tat-trasformazzjoni

4.1.4. Jikkoordina azzjonijiet legali, operattivi jew relatati mal-fornituri f'każ ta' ksur

4.2. Fornitur ta' Appoġġ tal-IT / IT Intern

4.2.1. Jagħżel u jimmaniġġja għodod ta' masking jew psewdonimizzazzjoni

4.2.2. Jiżgura li jiġu applikati metodi xierqa ta' trasformazzjoni skont it-tip ta' data

4.2.3. Iżomm logs ta' settijiet tad-data trasformati u proċeduri għall-ġestjoni taċ-ċwieviet

4.2.4. Jiżgura li l-masking isir qabel l-użu għal test, minn fornituri jew għall-analitika

[... Is-sezzjonijiet 4.3–8 mhumiex inklużi f'dan il-preview. Ixtri d-dokument sħiħ biex taċċessa l-kontenut kollu. ...]

9. Rekwiżiti għar-rieżami u l-aġġornament

9.1. Rieżami annwali

9.1.1. Din il-politika għandha tiġi rieżaminata mill-inqas darba fis-sena mill-Maniġer Ġenerali sabiex jiġi żgurat li tirrifletti:

9.1.1.1. Aġġornamenti fir-regolamenti applikabbli (eż. GDPR, DORA)

9.1.1.2. Sistemi godda tan-negozju jew skambji tad-data ma' partijiet terzi

9.1.1.3. Feedback minn awditi jew incidenti li jinvolvu użu ta' data mingħajr masking

9.2. Rieżamijiet interim

9.2.1. Ir-rieżamijiet għandhom isiru wkoll meta:

9.2.1.1. Jiġu introdotti applikazzjonijiet jew pjattaformi godda li jimmaniġġjaw data sensitiva

9.2.1.2. Incident ewlieni jiżvela lakuni fil-kontrolli attwali tat-trasformazzjoni

9.2.1.3. Bidliet fil-livelli ta' klassifikazzjoni jaffettwaw il-proċeduri tal-immaniġġjar tad-data

9.3. Kontroll tal-verżjoni u ġestjoni tat-tibdil

9.3.1. Il-bidliet kollha fil-politika għandhom ikunu:

9.3.1.1. Approvati mill-GM u dokumentati f'log tat-tibdil

9.3.1.2. Ikkomunikati b'mod ċar lill-impjegati u lill-fornituri tas-servizzi affettwati

9.3.1.3. Arkivjati b'mod sigur b'aċċess ristrett għal verżjonijiet skaduti

10. Politiki relatati u rabtiet

10.1. Din il-politika għandha tiġi applikata flimkien mal-politiki SME li ġejjin sabiex tiġi żgurata protezzjoni konsistenti u vinkolanti tad-data sensitiva:

10.1.1. P13S – Politika dwar il-Klassifikazzjoni u t-Tikkettar tad-Data: Tiddefinixxi l-livelli ta' klassifikazzjoni (eż. Kunfidenzjali – Personali) li jiddeterminaw meta għandu jiġi applikat il-masking jew il-pseudonimizzazzjoni. Din il-politika timponi regoli ta' trasformazzjoni bbażati fuq il-livelli ta' sensitività tad-data.

10.1.2. P14S – Politika ta' Żamma u Rimi tad-Data: Tiżgura li settijiet tad-data trasformati, inklużi backups li fihom data masked jew pseudonimizzata, jinżammu u jintremew skont ir-regoli applikabbli, inkluż it-tħassir taċ-ċwieviet tal-mapping meta ma jibqgħux meħtieġa.

10.1.3. P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tallinja l-prattiki ta' trasformazzjoni ma' obbligi usa' ta' privatezza, inklużi r-rekwiżiti tal-GDPR għall-minimizzazzjoni tad-data u l-użu tal-pseudonimizzazzjoni bħala salvagwardja għall-ipproċessar ta' data personali.

10.1.4. P30S – Politika dwar ir-Rispons għall-Inċidenti: Tkopri l-proċeduri ta' rappurtar u eskalazzjoni f'każ ta' żvelar mhux awtorizzat ta' data, inkluż l-użu mhux xieraq jew ir-riversjoni ta' data masked jew pseudonimizzata.

10.1.5. P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tassenja r-responsabbiltà ġenerali għall-implimentazzjoni tal-politika, l-aċċettazzjoni tar-riskju u l-approvazzjoni tal-eċċezzjonijiet, primarjament lill-Maniġer Ġenerali.

10.2. Dawn il-politiki jiffurmaw qafas integrat għall-protezzjoni tad-data u jiżguraw li l-isforzi ta' masking u pseudonimizzazzjoni jappoġġjaw iċ-ċertifikazzjoni ISO 27001 u l-konformità ma' oqfsa regolatorji differenti.

11. Standards u oqfsa ta' referenza

11.1. ISO/IEC 27001

11.1.1. Klawżola 6.1.3: Teħtieġ it-trattament tar-riskji għas-sigurtà tal-informazzjoni, li jinkludi l-mitigazzjoni tal-espożizzjoni permezz ta' tekniki ta' trasformazzjoni tad-data.

11.1.2. Klawżola 8.1: Tobbliga l-implimentazzjoni tal-kontrolli meħtieġa biex jintlaħqu l-oġettivi tas-sigurtà, inklużi l-pseudonimizzazzjoni u l-masking.

11.2. ISO/IEC 27002

11.2.1. Kontroll 8.11: Jipprovdni gwida dwar il-masking ta' data sensitiva f'sistemi ta' test u ta' żvilupp.

11.2.2. Kontroll 8.12: Joffri strateġiji sabiex tiġi evitata tnixxija tad-data permezz ta' trasformazzjoni kkontrollata u Prattiki ta' aċċess.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Jiżgura l-kunfidenzjalità tal-informazzjoni permezz ta' oskurement tad-data.

11.3.2. SC-28: Jipproteġi d-data maħżuna u d-data waqt l-użu.

11.3.3. PT-2/PT-3: Jippromwovu l-użu ta' teknoloġiji li jsaħħu l-privatezza, inkluża l-pseudonimizzazzjoni, meta tiġi pproċessata informazzjoni identifikabbli personalment (PII).

11.4. GDPR tal-UE

11.4.1. Artikolu 4(5): Jiddefinixxi legalment il-pseudonimizzazzjoni u jobbliga kontrolli fuq iċ-ċwieviet tal-mapping u l-identifikaturi.

11.4.2. Artikolu 5(1)(c): Jappoġġja l-prinċipji tal-minimizzazzjoni tad-data permezz tal-masking.

11.4.3. Artikolu 32: Jagħraf il-pseudonimizzazzjoni bħala kontroll tekniku li jnaqqas ir-riskji għall-privatezza.

11.5. Direttiva NIS2 tal-UE

11.5.1. Artikolu 21(2)(c): Tehtieg miżuri tekniċi proporzjonati biex jiġi minimizzat ir-riskju għas-sigurtà tad-data, inkluża l-psewdonimizzazzjoni bħala parti mill-kontroll tar-riskju.

11.6. DORA tal-UE

11.6.1. Artikolu 10(1): Tobbliga kontrolli tar-riskju relatati mal-ICT li jinkludu salvagwardji ta' trasformazzjoni tad-data għall-kontinwità u l-kunfidenzjalità waqt l-esternalizzazzjoni u l-iżvilupp tas-sistemi.

11.7. COBIT 2019

11.7.1. DSS05.01: Jehtieg il-protezzjoni tal-assi tal-informazzjoni, inkluża t-trasformazzjoni fejn possibbli.

11.7.2. DSS06.06: Jitlob tekniki xierqa ta' oskurement u psewdonimizzazzjoni biex tiġi limitata l-espożizzjoni tad-data f'ambjenti b'livell aktar baxx ta' fiduċja.