					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: P16					Titlu tad-dokument: **Politika dwar il-Masking tad-Data u l-Psewdonimizzazzjoni**						
Verżjoni: 1.0		Data tad-dħul fis-seħħ: 01.01.2025			Sid tad-dokument:						
X	Politika		Standard		Proċedura		Formola		Reġistru		Oħra

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

Approvazzjonijiet			
Isem	**Pożizzjoni**	**Data**	**Firma**

Allinjata ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżola 6.1	Rekwiżiti ġenerali għall-ġestjoni tar-riskju u għall-kontrolli operattivi għall-masking u l-psewdonimizzazzjoni
ISO/IEC 27002:2022	Kontrolli 8.11, 8	Gwida dwar il-kontrolli għall-implimentazzjoni tal-masking u l-psewdonimizzazzjoni
GDPR tal-UE	Artikoli 4(5), 5(1)(c,f), 32	Bażi legali u rekwiżiti għall-psewdonimizzazzjoni u għall-miżuri ta’ protezzjoni tad-data
Direttiva NIS2 tal-UE	Artikolu 21(2)(c)	Obbligu għal miżuri tekniċi u organizzattivi, inklużi teknoloġiji li jsaħħu l-privatezza (PETs)
DORA tal-UE	Artikoli 10(1), 10(2)(e)	Ġestjoni tar-riskju tal-ICT u kontrolli ta’ kunfidenzjalità għall-masking u l-psewdonimizzazzjoni tad-data
COBIT 2019	DSS05.01, DSS06.06, MEA	Kontrolli ta’ governanza għall-protezzjoni tad-data bl-użu tal-masking u l-evalwazzjoni tal-konformità

1. Għan

1.1 Din il-politika tiddefinixxi l-approċċ tal-organizzazzjoni għall-implimentazzjoni tal-masking tad-data u tal-psewdonimizzazzjoni bħala teknoloġiji li jsaħħu l-privatezza (PETs), sabiex tnaqqas l-identifikabbiltà u l-espożizzjoni ta’ data personali jew sensittiva.

1.2 Hija tappoġġa l-użu sigur tal-informazzjoni fl-ittestjar, fl-analitika u fl-operazzjonijiet, filwaqt li tiżgura konformità mar-rekwiżiti legali u regolatorji, timmitiga l-impatt ta’ ksur tad-data u ssaħħaħ il-prinċipji tal-minimizzazzjoni tad-data u tal-kunfidenzjalità.

1.3 Il-politika hija allinjata ma’ ISO/IEC 27001:2022, tappoġġa l-Artikolu 4(5) tal-GDPR dwar il-psewdonimizzazzjoni, u tintegra implimentazzjoni bbażata fuq ir-riskju konsistenti mal-istandards ta’ NIST, NIS2, DORA u COBIT 2019.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-impjegati, il-kuntratturi, il-partijiet terzi u l-fornituri kollha b’aċċess għal sistemi li jimmaniġġjaw informazzjoni personali, kunfidenzjali jew sensittiva.

2.1.2 L-ambjenti kollha tad-data, inklużi l-produzzjoni, l-iżvilupp, l-ittestjar u l-ambjent ta’ staging.

2.1.3 Il-forom kollha ta’ masking tad-data (eż. statiku, dinamiku, deterministiku, tokenization) u t-tekniki ta’ psewdonimizzazzjoni użati biex jitnaqqsu r-riskji għall-privatezza.

2.1.4 It-tipi kollha ta’ data (strutturata jew mhux strutturata), sistemi (fuq il-post jew ospitati fil-cloud) u applikazzjonijiet li jinvolvu data personali jew data rregolata.

2.2 Il-kamp ta’ applikazzjoni jinkludi l-użu fi:

2.2.1 Żvilupp ta’ applikazzjonijiet u ambjenti ta’ assigurazzjoni tal-kwalità (QA)/ittestjar

2.2.2 Pjattaformi ta’ analitika jew rapportar

2.2.3 Skambji tad-data ma’ partijiet terzi jew fornituri tas-servizzi

2.2.4 Sistemi ta’ backup, arkivjar jew irkupru

3. Objettivi

3.1 Tiżgura applikazzjoni konsistenti u effettiva tal-masking u tal-psewdonimizzazzjoni biex jitnaqqsu r-riskji ta’ espożizzjoni tad-data jew ta’ użu ħażin tagħha.

3.2 Tiżgura li data reali qatt ma tintuża f’ambjent mhux ta’ produzzjoni sakemm ma tkunx ġiet trasformata permezz ta’ tekniki PET approvati.

3.3 Iżżomm l-integrità referenzjali, l-użabbiltà u t-trasformazzjonijiet li jżommu l-format meta dawn ikunu meħtieġa għall-konsistenza operattiva.

3.4 Timplimenta kontrolli stretti tal-aċċess għad-data oriġinali, għad-data masked u għaċ-ċwievet tar-riidentifikazzjoni.

3.5 Tittratta s-settijiet ta’ data masked jew psewdonimizzati bħala data sensittiva, soġġetti għal logging tal-aċċess, kontrolli ta’ żamma u protokolli ta’ rispons għall-inċidenti.

3.6 Tivverifika l-effettività ta’ dawn il-kontrolli permezz ta’ ttestjar kontinwu, monitoraġġ u proċeduri ta’ awditjar.

4. Rwoli u responsabbiltajiet

4.1 Maniġment Eżekuttiv

4.1.1 Japprova din il-politika u jiżgura l-applikazzjoni tagħha bħala parti minn inizjattivi usa’ ta’ governanza tal-IT u ta’ protezzjoni tad-data.

4.2 Uffiċjal Ewlieni tas-Sigurtà tal-Informazzjoni (CISO) / Maniġer tal-ISMS

4.2.1 Jissorvelja l-implimentazzjoni u l-konformità kontinwa.

4.2.2 Jiżgura allinjament mal-Klawżola 6.1.3 ta’ ISO/IEC 27001 (trattament tar-riskju) u mal-Klawżola 8.1 (kontroll operattiv).

4.2.3 Jirrevedi l-logs tal-awditjar u jivverifika l-effettività tal-kontrolli.

[... 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 Din il-politika għandha tiġi rieżaminata mill-inqas darba fis-sena jew qabel jekk iseħħ wieħed minn dawn li ġejjin:

9.1.1 Bidliet regolatorji li jaffettwaw il-masking jew il-psewdonimizzazzjoni

9.1.2 Adozzjoni ta’ sistemi ġodda tal-IT li jimmaniġġjaw data sensittiva

9.1.3 Bidliet materjali fl-iskema tal-klassifikazzjoni tad-data tal-organizzazzjoni

9.1.4 Sejbiet tal-awditjar li jindikaw nuqqasijiet fil-kontrolli

9.1.5 Emerġenza ta’ theddid ġdid jew teknoloġiji ġodda ta’ masking

9.2 Il-Maniġer tal-ISMS għandu jmexxi r-rieżami b’konsultazzjoni mad-DPO, mas-Sidien tad-Data, mas-Sigurtà tal-IT u mal-Legali. L-aġġornamenti għandhom ikunu taħt kontroll tal-verżjoni, approvati mit-Tmexxija Eżekuttiva u kkomunikati lill-partijiet interessati kollha affettwati.

10. Politiki relatati u rabtiet

10.1 P13 - Politika dwar il-Klassifikazzjoni u t-Tikkettar tad-Data. Id-deċiżjonijiet dwar il-masking u l-psewdonimizzazzjoni jiddependu direttament mill-klassifikazzjoni tal-kampi tad-data u mil-livelli ta’ sensittività definiti f’P13.

10.2 P14 - Politika taż-Żamma tad-Data u r-Rimi. Settijiet ta' data trasformata għandhom jinżammu u jintremew skont ir-regoli taċ-ċiklu tal-ħajja f'P14, sabiex jiġi żgurat li data masked u psewdonimizzata tiġi trattata bħala sensittiva.

10.3 P17 - Politika dwar il-Protezzjoni tad-Data u l-Privatezza. Tipprovdi l-prinċipji tal-privatezza u l-bażijiet regolatorji għall-applikazzjoni tal-psewdonimizzazzjoni bħala attività ta' pproċessar konformi taħt il-GDPR u liġijiet simili.

10.4 P22 - Politika tal-Logging u l-Monitoraġġ. Tippermetti awditjar u twissijiet ċentralizzati ta' avvenimenti ta' masking u psewdonimizzazzjoni skont protokolli strutturati ta' monitoraġġ tas-sigurtà.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 6.1.3 - Pjan ta' Trattament tar-Riskju: Tistabbilixxi l-masking u l-psewdonimizzazzjoni bħala mekkaniżmi ta' trattament tar-riskju biex titnaqqas l-identifikabbiltà ta' data sensittiva f'ambjenti ta' pproċessar mhux essenzjali.

11.1.2 Klawżola 8.1 - Ippjanar u Kontroll Operattiv: Teħtieġ kontrolli tekniċi u proċedurali għal trasformazzjoni sigura tad-data waqt l-ipproċessar, il-ħażna jew it-trasferiment.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrolli 8.11, 8: Gwida dwar il-masking tad-data u l-psewdonimizzazzjoni biex jitnaqqsu r-riskji ta' riidentifikazzjoni u tnixxija ta' data.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Protezzjoni tal-PII: Implimentazzjoni ta' teknoloġiji li jsaħħu l-privatezza bħall-masking u l-psewdonimizzazzjoni.

11.3.2 PT-2, PT-3: Minimizzazzjoni u Sigurtà tal-Ipproċessar tal-PII - Trasformazzjoni biex titnaqqas l-identifikabbiltà u jiġi infurzat il-kontroll tal-aċċess.

11.3.3 SC-12, SC-28, SC-30: Kunfidenzjalità u Integrità tad-Data - Kontrolli ta' kunfidenzjalità u ta' oskurament għall-ħażna, it-trasmissjoni u l-użu.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikolu 4(5): Definizzjoni formali tal-psewdonimizzazzjoni.

11.4.2 Artikolu 32: Sigurtà tal-ipproċessar - miżuri organizzattivi u tekniċi għall-psewdonimizzazzjoni.

11.4.3 Artikolu 5(1)(c,f): Minimizzazzjoni tad-data u kunfidenzjalità bl-użu tal-psewdonimizzazzjoni/masking.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(c): Teħtieġ PETs bħall-masking u l-psewdonimizzazzjoni bħala miżuri ta' sigurtà.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 10(1): Il-qafas tal-ġestjoni tar-riskju tal-ICT jinkludi kontrolli ta' masking u psewdonimizzazzjoni.

11.6.2 Artikolu 10(2)(e): Jeħtieġ l-użu ta' teknoloġiji ta' trasformazzjoni biex jipproteġu data personali u finanzjarja.

11.7 COBIT 2019

11.7.1 DSS05.01: Ipproteġi l-assi tal-informazzjoni - Rekwiżiti għall-masking u l-psewdonimizzazzjoni.

11.7.2 DSS06.06: Ittestjar u Analitika Siguri - Masking f'ambjenti barra mill-produzzjoni.

11.7.3 MEA03: Monitoraġġ tal-konformità għall-effettività tal-masking u tal-psewdonimizzazzjoni.