					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P17					Titlu tad-dokument: **Politika dwar il-Protezzjoni tad-Data u l-Privatezza**							
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	Klawżoli 5.1, 6.1.3, 8.1, 10	Kontrolli ġenerali, tekniċi u ta’ titjib kontinwu rilevanti għall-protezzjoni tad-data
ISO/IEC 27002:2022	Kontrolli 5.34, 8.10, 8.11, 8.12	Kontrolli għall-immaniġġjar tal-PII, iż-żamma, it-tħassir, l-anonimizzazzjoni u d-drittijiet tas-suġġett tad-data
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Rekwiżiti ta’ governanza, riskju, ġestjoni tal-aċċess, logging, rispons għal ksur u programm tal-privatezza
GDPR tal-UE	Artikoli 5, 6, 12–23, 25, 28, 30, 32–34; Premessa 78	Il-prinċipji ewlenin kollha tal-privatezza, ir-responsabbiltà, id-drittijiet tas-suġġett tad-data, DSRs, ksur, u l-prinċipji tal-protezzjoni tad-data mid-disinn u b’mod predefinit
Direttiva NIS2 tal-UE	Artikolu 21(2)(e), (f)	Kontrolli tas-sigurtà bbażati fuq ir-riskju għal entitajiet essenzjali u importanti
DORA tal-UE	Artikoli 6(2)(d), 11(1)(c), 15(1), 17	Governanza, riskju ta’ partijiet terzi u skadenzi għall-ipproċessar sigur
COBIT 2019	APO12, DSS01, DSS05, MEA	Ġestjoni tar-riskju, operazzjonijiet siguri u monitoraġġ tal-konformità

1. Għan

1.1 Din il-politika tistabbilixxi prinċipji organizzattivi obbligatorji u rekwiżiti tekniċi għall-protezzjoni tad-data personali u għall-applikazzjoni tal-prinċipju tal-privatezza mid-disinn fl-ambjenti kollha.

1.2 Din tifformalizza r-responsabbiltajiet tal-organizzazzjoni skont standards internazzjonali u oqfsa regolatorji, filwaqt li tiżgura li d-data personali tinġabar, tiġi pproċessata, tinżamm, tinqasam u tintrema b’mod legali, sigur u trasparenti.

1.3 Din il-politika ssaħħaħ ukoll il-konformità mal-liġijiet u l-oqfsa applikabbli dwar il-privatezza, inkluż il-GDPR tal-UE, id-Direttiva NIS2 tal-UE, id-DORA tal-UE, l-ISO/IEC 27001:2022 u l-COBIT 2019.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għall-unitajiet organizzattivi, il-persunal u s-sistemi kollha involuti fl-ipproċessar ta’ data personali, inklużi:

2.1.1 Impjegati, kuntratturi, konsulenti u fornituri ta’ servizzi terzi.

2.1.2 Data miġbura minn sorsi interni u esterni fil-funzjonijiet kollha tan-negozju.

2.1.3 Mezzi fiżiċi u diġitali, inklużi servizzi cloud, pjattaformi SaaS, apparati mobbli u reġistri bbażati fuq il-karta.

2.1.4 L-ambjenti kollha, inklużi sistemi ta’ produzzjoni, żvilupp, test u backup fejn jista’ jkun hemm data personali.

2.2 Din tkopri l-attivitajiet kollha tal-ipproċessar regolati mil-liġijiet u l-istandards applikabbli dwar il-privatezza, inklużi iżda mhux limitati għal:

2.2.1 Il-ġbir, il-ħażna, l-użu, it-trażmissjoni u r-rimi ta' data personali.

2.2.2 L-eżerċizzju tad-drittijiet tas-suġġett tad-data, id-dokumentazzjoni tal-bażi legali u l-ġestjoni tal-kunsens.

2.2.3 Trasferimenti transkonfinali, notifika ta' ksur u qsim ta' data ma' partijiet terzi.

2.2.4 Disinn sigur u applikazzjoni tal-privatezza b'mod predefinit fis-sistemi u fil-proċessi.

3. Objettivi

3.1 Tiżgura pproċessar legali, trasparenti u responsabbli tad-data personali f'allinjament mal-ISO/IEC 27001:2022 u mar-rekwiżiti legali assoċjati.

3.2 Tintegra l-prinċipji tal-privatezza mid-disinn u tal-privatezza b'mod predefinit fis-sistemi tal-informazzjoni, is-servizzi u l-proċessi tan-negozju kollha.

3.3 Tapplika miżuri tekniċi u organizzattivi (TOMs) li jipproteġu l-kunfidenzjalità, l-integrità u d-disponibbiltà (CIA) tad-data personali tul iċ-ċiklu tal-ħajja tagħha.

3.4 Tiddefinixxi rwoli ta' governanza u strutturi ta' responsabbiltà għall-protezzjoni tad-data, inklużi r-responsabbiltajiet tal-Uffiċjal tal-Protezzjoni tad-Data (DPO), tas-Sigurtà tal-Informazzjoni, tal-funzjoni Legali u tas-Sidien tad-Data.

3.5 Tippermetti konformità sħiħa mal-Artikoli 5, 6, 25, 30 u 32 tal-GDPR, kif ukoll mar-rekwiżiti ta' mitigazzjoni tar-riskju u reżiljenza skont in-NIS2 u d-DORA.

3.6 Tħares id-drittijiet tas-suġġett tad-data, inkluż l-aċċess, ir-rettifika, it-tħassir, ir-restrizzjoni, il-portabbiltà, l-oġġezzjoni u l-protezzjoni minn teħid ta' deċiżjonijiet awtomatizzat.

3.7 Tnaqqas ir-riskji regolatorji, reputazzjonali, legali u operattivi li jirriżultaw minn aċċess mhux awtorizzat, użu ħażin jew telf ta' data personali.

4. Rwoli u responsabbiltajiet

4.1 Maniġment Eżekuttiv

4.1.1 Jipprovdi sorveljanza strateġika u jalloka riżorsi suffiċjenti biex isostni l-programm tal-privatezza.

4.1.2 Japprova din il-politika u jiżgura l-implimentazzjoni tagħha fl-organizzazzjoni kollha.

4.2 Uffiċjal tal-Protezzjoni tad-Data (DPO)

4.2.1 Jaġixxi b'mod indipendenti biex jissorvelja l-konformità mar-regolamenti dwar il-protezzjoni tad-data.

4.2.2 Iżomm ir-Record of Processing Activities (RoPA) skont l-Artikolu 30 tal-GDPR.

4.2.3 Imexxi l-involviment mar-regolaturi, iwettaq Data Protection Impact Assessments (DPIAs), u jimmaniġġja l-proċessi ta' notifika tal-ksur.

4.2.4 Jirrevedi eċċezzjonijiet relatati mal-privatezza u jżomm ir-Reġistru tal-Eċċezzjonijiet tal-Privatezza.

[... 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 kull sena jew qabel, taħt il-kundizzjonijiet li ġejjin:

9.1.1 Aġġornamenti legali jew regolatorji sinifikanti (eż. emendi għall-GDPR, skadenzi tad-DORA)

9.1.2 Sistemi jew attivitajiet ġodda ta' pproċessar li jinvolvu data personali

9.1.3 Sejbiet tal-awditjar intern li jindikaw lakuni fil-politika

9.1.4 Inċidenti materjali ta' ksur jew feedback mill-awtorità superviżorja

9.2 Responsabbiltajiet tar-rieżami

9.2.1 Id-DPO għandu jibda r-rieżami tal-politika, b'koordinazzjoni mal-funzjonijiet Legali, tar-Riskju, tas-Sigurtà tal-Informazzjoni u tal-Maniġment Eżekuttiv.

9.2.2 L-aġġornamenti kollha għandhom jiġu rreġistrati fir-Reġistru tal-Kontroll tad-Dokumenti tal-ISMS u mqassma lill-partijiet interessati affettwati.

9.3 Kontroll tat-tibdil

9.3.1 Kull reviżjoni ta' din il-politika għandha tiġi approvata formalment mill-Maniġment Eżekuttiv.

9.3.2 Verżjonijiet obsoleti għandhom jiġu arkivjati b'mod sigur, u l-verżjoni aġġornata għandha tinkludi storja dokumentata tat-tibdil.

10. Politiki relatati u rabtiet

10.1 P1 – Politika tas-Sigurtà tal-Informazzjoni. Tistabbilixxi l-prinċipji ġenerali ta' governanza tas-sigurtà li fuqhom hija bbażata din il-politika tal-privatezza. P1 tappoġġja l-kunfidenzjalità, l-integrità u d-disponibbiltà (CIA) tad-data personali fis-sistemi u s-servizzi kollha.

10.2 P6 – Politika tal-Ġestjoni tar-Riskju. Tiddefinixxi l-metodoloġija tal-organizzazzjoni għat-trattament tar-riskju, li hija essenzjali għall-evalwazzjoni tar-riskji tal-privatezza, il-proċessi tad-DPIA u l-evalwazzjonijiet tar-riskju residwu meħtieġa skont il-GDPR u l-Klawżola 6.1.3 tal-ISO/IEC 27001.

10.3 P13 – Politika dwar il-Klassifikazzjoni u t-Tikkettar tad-Data. Tiggwida l-kategorizzazzjoni ta' data personali u sensittiva, u tifforma l-bażi għall-applikazzjoni ta' kontrolli xierqa tal-privatezza inklużi ż-żamma, il-limitazzjoni tal-aċċess u r-rimi sigur.

10.4 P14 – Politika taż-Żamma u r-Rimi tad-Data. Tappoġġja direttament ir-rekwiżiti tal-privatezza skont l-Artikoli 5(1)(e) u 17 tal-GDPR, billi tiżgura li d-data personali tinżamm biss għal kemm ikun meħtieġ u tintrema b'mod sigur skont l-obbligi legali.

10.5 P16 – Politika dwar il-Masking tad-Data u l-Psewdonimizzazzjoni. Tistabbilixxi kontrolli biex titnaqqas l-identifikabbiltà tad-data personali permezz ta' miżuri tekniċi bħat-tokenization, masking dinamiku u psewdonimizzazzjoni, u b'hekk tapplika l-Artikolu 32 tal-GDPR u l-Kontroll 5.34 tal-ISO/IEC 27002.

10.6 P30 – Politika dwar ir-Rispons għall-Inċidenti. Tiddeskrivi l-protokolli obbligatorji ta' rispons għall-ksur li jintegraw mal-immaniġġjar tal-ksur tal-privatezza u mal-iskadenzi tan-notifika meħtieġa skont l-Artikoli 33 u 34 tal-GDPR.

10.7 P33 – Politika tal-Monitoraġġ tal-Awditjar u l-Konformità. Tistabbilixxi evalwazzjonijiet skedati tal-effettività tal-programm tal-privatezza, l-implimentazzjoni tal-politika u t-traċċar tal-azzjonijiet korrettivi fl-unitajiet organizzattivi u fost il-proċessuri terzi.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 5.1 – Tmexxija u Impenn: Tistabbilixxi responsabbiltà fil-livell eżekuttiv għall-protezzjoni tad-data personali u għall-applikazzjoni tal-prinċipji tal-privatezza.

11.1.2 Klawżola 6.1.3 – Trattament tar-Riskju tas-Sigurtà tal-Informazzjoni: Tappoġġja l-identifikazzjoni, l-evalwazzjoni u t-trattament tar-riskju tal-privatezza permezz ta' DPIAs u eċċezzjonijiet.

11.1.3 Klawżola 8.1 – Ippjanar u Kontroll Operattiv: Teħtieġ salvagwardji tekniċi u proċedurali biex jiġi żgurat li d-data personali tiġi pproċessata b'mod sigur.

11.1.4 Klawżola 10.1 – Titjib Kontinwu: Tistabbilixxi evalwazzjoni perjodika u adattament tal-programm tal-privatezza.

11.2 Kontrolli 5.34, 8.10, 8.11, 8.12 tal-ISO/IEC 27002:2022: Jipprovdu gwida dwar l-immaniġġjar tal-PII, l-applikazzjoni taż-żamma, it-tħassir, l-anonimizzazzjoni u t-trasparenza fir-rigward tad-drittijiet tas-suġġett tad-data.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: Jiddefinixxu governanza, rwoli, accountability u responsabbiltajiet ta' taħriġ dwar il-privatezza.

11.3.2 PL-2, PL-8: Jeħtieġu l-integrazzjoni tal-kontrolli tal-privatezza fiċ-ċiklu tal-ħajja tas-sistema u fl-arkitettura tal-intrapriża.

11.3.3 AC-2, AC-6: Japplikaw il-prinċipju tal-inqas privileġġ u l-ġestjoni tal-kontijiet għall-protezzjoni tad-data personali.

11.3.4 AU-2, AU-6, AU-9: Jeħtieġu logging, traċċabbiltà u integrità tal-awditjar għall-aċċess għad-data personali.

11.3.5 IR-4, IR-5, IR-6: Jiddefinixxu proċessi strutturati ta' skoperta, analiżi u rappurtar għal ksur tal-privatezza.

11.3.6 PM-1, PM-21, PM-23: Jistabbilixxu programm komprensiv tal-privatezza, allinjat mal-objettivi strateġiċi tar-riskju u tal-governanza tad-data.

11.4 GDPR tal-UE (2016/679)

11.4.1 Artikoli 5, 6, 12–23, 25, 28, 30, 32–34: Jirregolaw l-ipproċessar legali, il-limitazzjoni tal-għan, id-drittijiet tas-suġġett tad-data, ir-responsabbiltà, il-protezzjoni tad-data mid-disinn u b'mod predefinit, l-obbligi tal-partijiet terzi u l-ġestjoni tal-ksur.

11.4.2 Premessa 78: Issaħħaħ il-prinċipji tal-privatezza mid-disinn.

11.5 Direttiva NIS2 tal-UE (2022/2555)

11.5.1 Artikolu 21(2)(e) u (f): Jeħtieġ l-implimentazzjoni ta' kontrolli tas-sigurtà bbażati fuq ir-riskju u l-protezzjoni tad-data personali fi ħdan il-kamp ta' applikazzjoni ta' entitajiet essenzjali u importanti.

11.6 DORA tal-UE (2022/2554)

11.6.1 Artikolu 6(2)(d): Jistabbilixxi governanza interna għar-riskju tal-ICT relatat mal-immaniġġjar tad-data.

11.6.2 Artikolu 11(1)(c): Jeħtieġ sorveljanza tar-riskju ta' partijiet terzi għal servizzi relatati mad-data.

11.6.3 Artikoli 15(1) u 17: Jeħtieġu pproċessar sigur tad-data mill-forniturі tas-servizzi u żvelar superviżorju f'waqtu wara inċidenti relatati mal-ICT.

11.7 COBIT 2019

11.7.1 APO12 – Ġestjoni tar-Riskju: Tintegra r-riskju tal-privatezza fis-sorveljanza usa' tar-riskju tal-organizzazzjoni.

11.7.2 DSS01 – Operazzjonijiet Immaniġġjati u DSS05 – Servizzi ta' Sigurtà: Jiżguraw operazzjonijiet siguri inklużi kontroll tal-aċċess, żamma u integrità tas-sistema.

11.7.3 MEA03 – Monitoraġġ tal-Konformità: Jeħtieġ rieżami kontinwu tal-istatus tal-konformità kontra obbligi regolatorji u tal-privatezza bbażati fuq il-politiki.