					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P17S					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	
ISO/IEC 27002:2022	Kontrolli 5.34, 8.10–8	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
GDPR tal-UE	Artikolu 5, 6, 12-23, 30, 32-34	
Direttiva NIS2 tal-UE	Artikolu 21(2)(e), 21(2)(f)	
DORA tal-UE	Artikoli 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Għan

1.1. Din il-politika tiddefinixxi kif l-organizzazzjoni tipproteġi d-data personali f’konformità mal-obbligi legali, l-oqfsa regolatorji u l-istandards internazzjonali tas-sigurtà.

1.2. Tiżgura li d-data personali — kemm jekk ta’ klijenti, persunal jew imsieħba — tinġabar, tintuża, tinħażen u titħassar b’mod legali, ġust u sigur.

1.3. Din il-politika tappoġġja wkoll il-konformità ma’ ISO/IEC 27001:2022 u ssaħħaħ il-kapaċità li tintwera l-konformità billi timponi approċċ konsistenti u bbażat fuq ir-riskju għall-protezzjoni tal-privatezza.

1.4. Permezz ta’ din il-politika, l-organizzazzjoni turi responsabbiltà u tibni l-fiduċja tal-klijenti billi tagħti prijorità lit-trasparenza, il-minimizzazzjoni tad-data u governanza robusta tal-privatezza.

2. Kamp ta’ applikazzjoni

2.1. Din il-politika tapplika għal:

2.1.1. L-impjegati, il-kuntratturi u l-fornituri tas-servizzi kollha li jkollhom aċċess għal data personali, jipproċessawha jew jimmaniġġjawha

2.1.2. Kull sistema, applikazzjoni jew post fejn tinħażen jew tiġi trażmessa d-data personali

2.1.3. Id-data personali kollha, kemm jekk maħżuna elettronikament, fuq karta, f’sistemi ospitati fil-cloud jew fuq apparati mobbli

2.2. Din il-politika tapplika għal data relatata ma’ klijenti, persunal, fornituri u kwalunkwe individwu identifikabbli ieħor.

2.3. Din il-politika tibqa’ tapplika irrispettivament minn jekk id-data tiġix ipproċessata internament jew minn fornituri ta’ servizzi ta’ partijiet terzi.

3. Objettivi

3.1. Tiżgura li d-data personali tiġi mmaniġġjata skont il-liġijiet tal-privatezza u l-istandards tas-sigurtà, inklużi l-GDPR, in-NIS2 u l-ISO 27001.

3.2. Tipproteġi d-data personali kontra aċċess mhux awtorizzat, użu ħażin, alterazzjoni jew telf permezz ta’ kontrolli tekniċi u organizzattivi ċari.

3.3. Tirrispetta d-drittijiet tal-privatezza tal-individwi, inkluż id-dritt ta’ aċċess, rettifika u tħassir tad-data tagħhom.

3.4. Tistabbilixxi rwoli u responsabbiltajiet ċari għall-protezzjoni tad-data fi ħdan l-organizzazzjoni.

3.5. Tiżgura l-minimizzazzjoni tad-data, iż-żamma sigura u t-tħassir f'waqtu fis-sistemi u l-proċessi kollha.

3.6. Tnaqqas ir-riskju ta' nuqqas ta' konformità, penali legali, dannu reputazzjonali jew telf ta' fiduċja tal-klijenti.

4. Rwoli u responsabbiltajiet

4.1. Maniġer Ġenerali (GM)

4.1.1. Japprova din il-politika u jiżgura li tiġi implimentata

4.1.2. Jipprovdi r-riżorsi meħtieġa għall-ġestjoni tar-riskji tal-privatezza u għar-rispons għall-inċidenti

4.1.3. Iġorr ir-responsabbiltà ġenerali għall-konformità mal-liġijiet u l-istandards tal-privatezza

4.2. Koordinatur tal-Privatezza (Intern jew Esternalizzat)

4.2.1. Iżomm reġistri tal-attivitajiet tal-ipproċessar tad-data

4.2.2. Jirrispondi għal talbiet tas-suġġetti tad-data u għal mistoqsijiet regolatorji

4.2.3. Jappoġġja l-valutazzjonijiet tar-riskju, it-taħriġ u l-implimentazzjoni tal-politika

4.2.4. Jiddokumenta każijiet ta' ksur u jinnotifika lill-awtoritajiet meta meħtieġ

[... 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. Rieżamijiet Skedati

9.1.1. Din il-politika għandha tiġi rieżaminata mill-inqas darba kull 12-il xahar mill-Koordinatur tal-Privatezza u approvata mill-Maniġer Ġenerali

9.1.2. Ir-rieżami għandu jivvaluta r-rilevanza tal-politika, l-allinjament regolatorju u l-effettività operattiva

9.2. Attivaturi għal Rieżami Interim

9.2.1. Aġġornamenti tal-politika għandhom jinbdew ukoll b'reazzjoni għal:

9.2.1.1. Liġijiet ġodda jew riveduti dwar il-protezzjoni tad-data (eż. GDPR, DORA)

9.2.1.2. Inċidenti tas-sigurtà jew ksur tal-privatezza li jinvolvu data personali

9.2.1.3. It-tnedija ta' sistemi, għodod jew servizzi ġodda li jipproċessaw data personali

9.2.1.4. Sejbiet materjali tal-awditjar jew rakkomandazzjonijiet tar-regolatur

9.3. Kontroll tat-Tibdil u Komunikazzjoni

9.3.1. Il-bidliet kollha fil-politika għandhom jiġu dokumentati formalment f'log tat-tibdil

9.3.2. Verżjonijiet riveduti għandhom jitqassmu lill-persunal kollu u lill-kuntratturi applikabbli

9.3.3. Verżjonijiet arkivjati għandhom jinżammu biex tinżamm traċċa tal-awditjar tal-konformità

10. Politiki relatati u rabtiet

10.1. Din il-politika topera flimkien ma' politiki oħra tal-SME biex toħloq qafas komprensiv u applikabbli tal-privatezza:

10.1.1. P13S – Politika dwar il-Klassifikazzjoni u t-Tikkettar tad-Data: Tiżgura li d-data personali tiġi kklassifikata b'mod xieraq sabiex il-protezzjoni tal-privatezza tkun tista' tiġi applikata skont ir-riskju.

10.1.2. P14S – Politika dwar iż-Żamma tad-Data u r-Rimi: Tipprovdi regoli ċari dwar kemm għandha tinżamm id-data personali u dwar il-metodi siguri għar-rimi tagħha meta tiskadi.

10.1.3. P16S – Politika dwar il-Masking tad-Data u l-Psewdonimizzazzjoni: Tispeċifika kif l-identifikaturi personali għandhom jiġu trasformati qabel ma d-data tintuża f'ambjent mhux ta' produzzjoni jew tinqasam esternament.

10.1.4. P30S – Politika dwar ir-Rispons għall-Inċidenti: Tkopri l-passi meħtieġa għar-rispons għal ksur tad-data, inkluża n-notifika lir-regolaturi u lill-individwi affettwati fiż-żmien meħtieġ.

10.1.5. P2S – Politika dwar ir-Rwoli u r-Responsabbiltajiet tal-Governanza: Tiċċara l-istruttura tar-responsabbiltà u r-rwoli tat-teħid tad-deċiżjonijiet li japplikaw għall-implimentazzjoni u s-sorveljanza tal-privatezza.

10.2. Dawn il-politiki relatati għandhom jiġu rieżaminati u applikati flimkien biex jiżguraw kopertura komprensiva tal-privatezza fis-sistemi, fost il-persunal u mal-fornituri.

11. Standards u oqfsa ta' referenza

11.1. ISO/IEC 27001

11.1.1. Klawżola 5.1 – Teħtieġ li t-Tmexxija Għolja turi tmexxija u impenn fil-protezzjoni tad-data personali.

11.1.2. Klawżola 6.1.3 – Teħtieġ it-trattament tar-riskji relatati mal-ipproċessar ta' informazzjoni personali.

11.1.3. Klawżola 8.1 – Teħtieġ l-implimentazzjoni ta' kontrolli operattivi biex tiġi protetta d-data tul iċ-ċiklu tal-ħajja tagħha.

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.34 – Jipprovdi gwida għall-implimentazzjoni dwar il-protezzjoni tal-privatezza u l-immaniġġjar sigur ta' informazzjoni identifikabbli personalment (PII).

11.2.2. Kontroll 8.10 – Jindirizza r-rimi sigur tad-data personali biex jiġi evitat żvelar residwu.

11.2.3. Kontroll 8.11 – Jappoġġja l-użu ta' masking u psewdonimizzazzjoni għall-minimizzazzjoni tad-data.

11.2.4. Kontroll 8.12 – Jipprevjeni tnixxija ta' data mhux awtorizzata permezz ta' kontrolli fuq l-aċċess għad-data u l-użu tagħha.

11.3. NIST SP 800-53 Rev.

11.3.1. AR-2 – Jassenja rwoli u responsabbiltajiet għall-ġestjoni tar-riskju tal-privatezza.

11.3.2. PL-5 – Teħtieġ dokumentazzjoni tal-pjan tal-privatezza li tkopri l-użu u l-protezzjoni tad-data.

11.3.3. AC-6 – Teħtieġ il-prinċipju tal-inqas privileġġ u kontrolli tal-aċċess għad-data personali.

11.3.4. IR-4 – Teħtieġ proċessi ta' ġestjoni tal-inċidenti għal ksur li jinvolvi data personali.

11.4. GDPR tal-UE

11.4.1. Artikolu 5 – Jiddefinixxi l-prinċipji ewlenin tal-ipproċessar legali, ġust u trasparenti tad-data.

11.4.2. Artikolu 6 – Jeħtieġ bażi legali valida għal kull attività ta' pproċessar ta' data personali.

11.4.3. Artikoli 12–23 – Jiddeskrivu d-drittijiet tas-suġġetti tad-data, inklużi l-aċċess, ir-rettifika, it-tħassir u l-oġġezzjoni.

11.4.4. Artikolu 30 – Jeħtieġ reġistri tal-attivitajiet tal-ipproċessar.

11.4.5. Artikolu 32 – Jeħtieġ miżuri tekniċi u organizzattivi xierqa ta' sigurtà.

11.4.6. Artikoli 33–34 – Jistabbilixxu obbligi ta' notifika ta' ksur lill-awtoritajiet u lis-suġġetti tad-data.

11.5. NIS2 tal-UE

11.5.1. Artikolu 21(2)(e) – Jeħtieġ miżuri biex tiġi żgurata l-protezzjoni tad-data allinjata mal-politiki taċ-ċibersigurtà.

11.5.2. Artikolu 21(2)(f) – Jeħtieġ mekkaniżmi biex tiġi ġestita s-sigurtà ta' data personali u kunfidenzjali fis-sistemi tal-ICT.

11.6. DORA tal-UE

11.6.1. Artikolu 6 – Jeħtieġ oqfsa interni ta' governanza li jimmaniġġjaw ir-riskju u l-protezzjoni tad-data.

11.6.2. Artikolu 15 – Jobbliga lill-entitajiet finanzjarji jiżguraw li l-fornituri ta' partijiet terzi jipproteġu d-data personali u jappoġġjaw il-konformità regolatorja.

11.6.3. Artikolu 17 – Jeħtieġ li l-organizzazzjonijiet jiżguraw li s-sistemi tal-ICT li jipproċessaw data personali jkunu siguri, reżiljenti u taħt monitoraġġ.

11.7. COBIT 2019

11.7.1. APO12 – Ġestjoni tar-Riskju: Jeħtieġ l-identifikazzjoni u t-trattament tar-riskji tal-privatezza u tal-protezzjoni tad-data.

11.7.2. DSS05 – Ġestjoni tas-Servizzi tas-Sigurtà: Jeħtieġ salvagwardji biex jipprevjenu aċċess mhux awtorizzat għal data personali.

11.7.3. MEA03 – Monitoraġġ tal-Konformità: Jeħtieġ li l-organizzazzjonijiet jiżguraw konformità kontinwa mal-liġijiet tal-privatezza u tal-protezzjoni tad-data.