					Daħħal hawn l-isem tal-entità ġuridika rreġistrata							
Numru tad-dokument: P37S					Titlu tad-dokument: **Politika Legali u Regolatorja dwar il-Konformità**							
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**

Allinjament ma’ standards u regolamenti

Standard/Regolament	Klawżola/Artikolu	Kumment
ISO/IEC 27001:2022	Klawżoli 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontroll 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
GDPR tal-UE	Artikoli 5, 6, 32, 33	
Direttiva NIS2 tal-UE	Artikoli 21(2)(a), 21(2)(f), 23	
DORA tal-UE	Artikoli 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Għan

1.1 Din il-politika tiddefinixxi l-approċċ tal-organizzazzjoni biex tidentifika, tikkonforma ma’, u turi l-osservanza tal-obbligi legali, regolatorji u kuntrattwali.

1.2 Hija tistabbilixxi responsabbiltajiet ċari u passi prattiċi biex tgħin lin-negozju jissodisfa l-obbligi ta’ konformità tiegħu, inklużi liġijiet dwar il-protezzjoni tad-data, oqfsa taċ-ċibersigurtà, ftehimiet mal-klijenti u standards ta’ ċertifikazzjoni.

1.3 Hija tiżgura li, anke mingħajr tim dedikat għall-konformità, in-negozju jkun jista’ jżomm operazzjonijiet konformi mal-liġi, jirrispondi b’mod xieraq għall-inċidenti, u jżomm il-kapaċità li juri l-konformità b’mod sħiħ.

1.4 Din il-politika hija essenzjali biex tappoġġa ċ-ċertifikazzjoni ISO/IEC 27001:2022 u biex tissodisfa l-aspettattivi esterni tal-klijenti, tar-regolaturi jew tas-sħab.

2. Kamp ta’ applikazzjoni

2.1 Din il-politika tapplika għal:

2.1.1 L-impjegati kollha, il-kuntratturi, il-freelancers u l-forniturі terzi kollha.

2.1.2 Is-servizzi, l-operazzjonijiet, is-sistemi u l-attivitajiet kollha ta’ mmaniġġjar tad-data fejn l-organizzazzjoni trid tissodisfa rekwiżiti legali jew kuntrattwali.

2.1.3 Il-postijiet u l-apparati kollha użati għall-ipproċessar ta’ informazzjoni tan-negozju, kemm jekk fl-uffiċċju, b’mod remot, jew ospitati fil-cloud.

2.2 Il-politika tkopri:

2.2.1 Liġijiet dwar il-protezzjoni tad-data bħall-GDPR tal-UE.

2.2.2 Regolamenti taċ-ċibersigurtà bħad-Direttiva NIS2 tal-UE.

2.2.3 Obbligi speċifiċi għas-settur, fejn applikabbli.

2.2.4 Kuntratti mal-klijenti, Ftehimiet ta’ Nuqqas ta’ Żvelar, u klawżoli ta’ awditjar.

2.2.5 Ċertifikazzjonijiet volontarji, pereżempju ISO 27001, u politiki interni li jridu jiġu applikati għall-konformità.

3. Objettivi

3.1 Tistabbilixxi r-responsabbiltà: Tassenja responsabbiltà ċara għall-monitoraġġ, l-aġġornament u l-applikazzjoni tal-obbligi legali, regolatorji u kuntrattwali.

3.2 Tipproteġi n-negozju: Timminimizza r-riskju ta’ ksur legali, multi, ksur tad-data u ħsara lir-reputazzjoni.

3.3 Tippermetti li tintwera l-konformità: Tżomm reġistri verifikabbli li juru kif l-organizzazzjoni tissodisfa l-obbligi ta’ konformità tagħha.

3.4 Tappoġġa l-integrazzjoni tal-politiki: Tiżgura li l-obbligi legali u regolatorji jiġu applikati b’mod konsistenti fil-politiki u l-proċessi kollha.

3.5 Tmexxi l-eċċezzjonijiet b’mod trasparenti: Tiżgura li kull eċċezzjoni għall-konformità tkun dokumentata, iġġustifikata u approvata sabiex tiġi evitata responsabbiltà legali.

4. Rwoli u responsabbiltajiet

4.1 Maniġer Ġenerali (GM)

4.1.1 Iġorr ir-responsabbiltà ġenerali għall-konformità legali u regolatorja tal-organizzazzjoni.

4.1.2 Iżomm ir-Reġistru tal-Konformità u jiżgura li jibqa’ aġġornat.

4.1.3 Jagħmel rieżami tal-kuntratti tal-klijenti u jiżgura li l-obbligi speċifiċi jiġu traċċati u applikati.

4.1.4 Japprova eċċezzjonijiet għall-obbligi ta’ konformità biss meta dawn ikunu legalment iġġustifikati u jkunu fis-seħħ kontrolli kumpensatorji.

4.2 Konsulenti esterni, pereżempju legali, tal-IT jew tal-konformità

4.2.1 Jappoġġaw lill-GM billi jidentifikaw il-liġijiet, iċ-ċertifikazzjonijiet u l-obbligi applikabbli, pereżempju GDPR, NIS2 u ISO 27001.

4.2.2 Jipprovdu gwida dwar kif għandhom jiġu interpretati regolamenti ġodda jew bidliet fil-liġijiet eżistenti.

4.2.3 Jistgħu jassistu fl-aġġornament tal-politiki, fl-awditi jew fir-rispons għal ksur meta jkun hemm espożizzjoni legali.

[... 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 skedat

9.1.1 Din il-politika għandha tiġi rieżaminata kull 12-il xahar mill-GM.

9.1.2 Ir-rieżami għandu jikkonferma:

9.1.2.1 Ir-rilevanza għall-kuntest legali u kuntrattwali attwali.

9.1.2.2 Ir-riflessjoni xierqa tal-ftehimiet mal-klijenti u tal-obbligi tas-servizz.

9.1.2.3 L-allinjament mar-Reġistru tal-Konformità u ma’ politiki oħra.

9.2 Aġġornamenti mmexxija minn avvenimenti

9.2.1 Huwa meħtieġ rieżami immedjat jekk:

9.2.1.1 Liġi jew regolament ġdid isir applikabbli, pereżempju rekwiżit ġdid dwar il-protezzjoni tad-data.

9.2.1.2 Klijent iżid termini kumplessi ta’ konformità mal-ftehim tiegħu.

9.2.1.3 Iseħħ ksur jew inċident ta’ nuqqas ta’ konformità.

9.2.1.4 Il-kumpanija tespandi f’suq jew settur regolat.

9.3 Approvazzjoni tal-aġġornamenti u kontroll tal-verżjoni

9.3.1 L-aġġornamenti kollha għandhom jiġu dokumentati, ivverżjonati u approvati mill-GM.

9.3.2 Verżjonijiet storiċi għandhom jinżammu għal skopijiet ta’ awditjar u legali.

9.4 Komunikazzjoni tat-tibdil

9.4.1 Il-persunal u l-kuntratturi għandhom jiġu infurmati dwar bidliet fil-politika fi żmien 5 ijiem tax-xogħol mill-approvazzjoni.

9.4.2 Kwalunkwe fornitur affettwat għandu wkoll jirrikonoxxi t-termini aġġornati qabel ma jkompli bit-twassil tas-servizz.

10. Politiki relatati u rabtiet

10.1 Din il-politika hija appoġġata u applikata permezz tal-politiki SME li ġejjin:

10.1.1 P3S – Politika dwar l-Użu Aċċettabbli: Tipprevjeni mġiba li tista' tikser termini legali jew kuntrattwali, pereżempju qsim ta' fajls mhux awtorizzat.

10.1.2 P8S – Politika dwar l-Għarfien tas-Sigurtà tal-Informazzjoni u t-Taħriġ: Teduka lill-persunal dwar l-obbligi ta' konformità u kif jevita ksur.

10.1.3 P14S – Politika ta' Żamma u Rimi tad-Data: Tiżgura prattiki legali għall-immaniġġjar tad-data matul iċ-ċiklu kollu tal-ħajja tad-data.

10.1.4 P17S – Politika dwar il-Protezzjoni tad-Data u l-Privatezza: Tissodisfa l-GDPR u r-rekwiżiti tal-klijenti dwar l-immaniġġjar tad-data.

10.1.5 P30S – Politika dwar ir-Rispons għall-Inċidenti: Tispjega kif għandu jsir ir-rispons għal ksur tad-data jew fallimenti fil-konformità, inkluży l-iskadenzi għan-notifika.

10.1.6 P36S – Politika dwar il-Midja Soċjali u l-Komunikazzjonijiet Esterni: Tiżgura li komunikazzjonijiet pubbliċi ma jiksrux obbligi legali jew regolatorji.

10.2 Kull politika marbuta tapplika parti mill-qafas tal-konformità legali u għandha tiġi applikata b'mod koordinat.

11. Standards u oqfsa ta' referenza

11.1 ISO/IEC 27001

11.1.1 Klawżola 6.1 – Azzjonijiet biex jiġu indirizzati r-riskji u l-opportunitajiet: Tinkludi riskji ta' konformità.

11.1.2 Klawżola 8.1 – Ippjanar u kontroll operattiv: Teħtieġ l-eżekuzzjoni ta' proċessi li jissodisfaw rekwiżiti legali u kuntrattwali.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.36 – Jiggwida lill-organizzazzjoni biex iżżomm reġistri tal-obbligi u tiżgura rispons xieraq għar-rekwiżiti legali u regolatorji.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politika u Proċeduri: Jeħtieġ politiki formali ta' konformità.

11.3.2 PM-1 – Pjan tal-Programm tas-Sigurtà tal-Informazzjoni: Jeħtieġ l-integrazzjoni tal-konformità legali fl-ippjanar tas-sigurtà.

11.3.3 CA-1 – Valutazzjoni, Awtorizzazzjoni u Monitoraġġ.

11.3.4 AU-1 – Politika tal-Awditjar: Teħtieġ iż-żamma ta' evidenza ta' konformità.

11.4 GDPR tal-UE

11.4.1 Artikolu 5 – Prinċipji tal-ipproċessar tad-data, inkluża r-responsabbiltà.

11.4.2 Artikolu 6 – Bażi legali għall-ipproċessar.

11.4.3 Artikolu 32 – Sigurtà tal-ipproċessar.

11.4.4 Artikolu 33 – Notifika ta' ksur fi żmien 72 siegħa.

11.5 Direttiva NIS2 tal-UE

11.5.1 Artikolu 21(2)(a) u (f) – Politiki interni għall-kontroll tar-riskju u għall-konformità regolatorja.

11.5.2 Artikolu 23 – Infurzar u penali għal fallimenti fil-konformità.

11.6 DORA tal-UE

11.6.1 Artikolu 5(2) – Sorveljanza maniġerjali tal-ġestjoni tar-riskju tal-ICT.

11.6.2 Artikolu 9(1) – Governanza interna tal-konformità.

11.6.3 Artikolu 17 – Arranġamenti kuntrattwali ma' fornituri ta' servizzi tal-ICT.

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: Jiżgura li r-riskji ta' konformità jiġu traċċati u indirizzati.

11.7.2 APO13 – Managed Security: Ikopri l-applikazzjoni bbażata fuq ir-riskju tal-konformità regolatorja u kuntrattwali.

11.7.3 DSS01 – Managed Operations: Jeħtieġ tħejjija operattiva biex jiġu ssodisfati l-obbligi legali.