					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: PII15					Titlu tad-dokument: **Politika għall-Ġestjoni ta' Inċidenti tal-PII u Ksur ta' Data Personali**						
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 / Kontroll / Artikolu	Applikabbiltà	Tip ta' kopertura	Kumment
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikazzjonijiet tal-PIMS u evidenza dokumentata ta' ksur
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Kontroll operattiv, valutazzjoni tar-riskju tal-privatezza, u rabta mat-trattament
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoraġġ, evalwazzjoni, nuqqas ta' konformità, azzjoni korrettiva, u titjib
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Ippjanar u tħejjija għall-ġestjoni tal-inċidenti għall-ipproċessar tal-PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Rispons għal inċidenti tas-sigurtà tal-informazzjoni li jinvolvu PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Rekwiżiti legali, statutorji, regolatorji u kuntrattwali, u protezzjoni tar-reġistri
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Ftehim tal-klijent tal-proċessur u appoġġ għall-obbligi tal-klijent
GDPR	Article 5(2); Article 24	Controller	Supporting	Responsabbiltà u responsabbiltà tal-kontrollur
GDPR	Article 26	Joint Controller	Supporting	Koordinazzjoni tar-responsabbiltà tal-kontrolluri konġunti għall-ksur
GDPR	Article 28	Both	Supporting	Assistenza tal-proċessur u obbligi kuntrattwali tal-proċessur

GDPR	Article 32	Both	Supporting	Sigurtà tal-ipproċessar u kapaċità ta' skoperta ta' ksur
GDPR	Article 33	Both	Primary	Notifika ta' ksur ta' data personali u dokumentazzjoni tal-ksur
GDPR	Article 34	Controller	Primary	Komunikazzjoni ta' ksur ta' data personali lill-prinċipali tal-PII affettwati
GDPR	Article 39	Conditional	Supporting	Parir tad-DPO, monitoraġġ, kooperazzjoni, u appoġġ bħala punt ta' kuntatt
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Prinċipji tas-sigurtà tal-informazzjoni u tal-konformità mal-privatezza
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Responsabbiltajiet tar-rispons għal inċidenti tal-PII u rappurtar ta' avvenimenti
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Ippjanar, evalwazzjoni, rispons, lessons learned, u ġbir tal-evidenza għall-inċidenti
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Ċiklu tal-ħajja tal-proċess tal-ġestjoni tal-inċidenti
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politika, pjan, sensibilizzazzjoni, ittestjar, u lessons learned dwar l-inċidenti
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operazzjonijiet ta' skoperta, notifika, triage, analiżi, rispons, u rappurtar
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Aspettattivi dwar notifika minn

				proċessur cloud u reġistri ta' ksur
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Rappurtar ta' inċidenti sinifikanti fejn applikabbli
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Ġestjoni, klassifikazzjoni u rappurtar ta' inċidenti tal-ICT fejn applikabbli

1. Kamp ta’ applikazzjoni

1.1 Din il-politika tiddefinixxi r-rekwiżiti għall-identifikazzjoni, ir-rappurtar, it-trijaġġ, l-evalwazzjoni, it-trażżin, in-notifika, id-dokumentazzjoni, l-għeluq u t-titjib minn inċidenti tal-PII u ksur ta’ data personali fi ħdan il-kamp ta’ applikazzjoni tal-PIMS.

1.2 Din il-politika tapplika għal:

1.2.1 l-organizzazzjoni meta taġixxi bħala kontrollur tal-PII;

1.2.2 l-organizzazzjoni meta taġixxi bħala kontrollur konġunt fejn tkun meħtieġa koordinazzjoni tar-responsabbiltà għall-ksur;

1.2.3 l-organizzazzjoni meta taġixxi bħala proċessur tal-PII;

1.2.4 l-organizzazzjoni meta taġixxi bħala subproċessur;

1.2.5 sistemi, applikazzjonijiet, servizzi, proċessi, forniturі, proċessuri, subprocessors, u partijiet terzi li jipproċessaw, jaħżnu, jittrażmettu, jappoġġaw, jaċċessaw, jew b’xi mod ieħor jaffettwaw PII fi ħdan il-kamp ta’ applikazzjoni tal-PIMS.

1.3 Din il-politika tuża REG10 - Reġistru tal-Inċidenti tal-PII u tal-Ksur ta’ Data Personali bħala l-oġġett ewlieni ta’ evidenza għall-ġestjoni ta’ inċidenti tal-PII u ksur ta’ data personali.

1.4 Din il-politika tuża oġġetti ta’ evidenza ta’ appoġġ kif ġej:

1.4.1 REG01 għall-kamp ta’ applikazzjoni tal-PIMS, u għall-kuntest applikabbli ta’ partijiet interessati, legali, kuntrattwali, settorjali u ta’ rappurtar lill-klijenti.

1.4.2 REG02 għall-attivitajiet ta’ pproċessar affettwati, il-kategoriji tal-PII, il-kategoriji ta’ prinċipali tal-PII, l-għanijiet u s-sistemi.

1.4.3 REG03 għad-Dikjarazzjoni ta’ Applikabbiltà u l-aġġornamenti tal-applikabbiltà tal-kontrolli.

1.4.4 REG04 għar-rabta mar-riskju tal-privatezza, mad-DPIA u mar-riskju residwu.

1.4.5 REG08 għall-evidenza tal-interfaċċa tal-inċidenti ma’ proċessuri, subproċessuri, klijenti, forniturі u partijiet terzi.

1.4.6 REG09 għar-rabta mat-trasferiment internazzjonali meta inċident jaffettwa pproċessar transkonfinali.

1.4.7 REG11 għall-evidenza tat-taħriġ, is-sensibilizzazzjoni u l-kompetenza fir-rispons għall-inċidenti.

1.4.8 REG12 għall-evidenza tal-awditjar, tan-nuqqas ta’ konformità, tal-azzjoni korrettiva u tat-titjib.

1.5 Din il-politika tiddependi fuq politiki relatati tal-PIMS għal kontrolli speċjalizzati:

1.5.1 PII03 tirregola l-inventarju tal-ipproċessar u r-reġistri tal-bażi legali.

1.5.2 PII04 tirregola l-avviż ta’ privatezza u l-kontrolli tat-trasparenza barra mill-komunikazzjonijiet speċifiċi għall-ksur.

1.5.3 PII06 tirregola t-talbiet dwar id-drittijiet tal-prinċipali tal-PII li jinqalgħu qabel, matul jew wara inċident.

1.5.4 PII07 tirregola l-metodoloġija tal-valutazzjoni tar-riskju tal-privatezza u tad-DPIA.

1.5.5 PII08 tirregola l-kontrolli tal-privatezza mid-disinn u b’mod predefinit.

1.5.6 PII10 tirregola l-kontrolli taż-żamma, it-tħassir u r-rimi.

1.5.7 PII12 tirregola l-kontrolli tar-relazzjonijiet ta’ privatezza ma’ proċessuri, subproċessuri, forniturі u partijiet terzi.

1.5.8 PII13 tirregola l-mekkaniżmi ta’ trasferiment internazzjonali tal-PII u r-reġistri tar-riskju tat-trasferiment.

1.5.9 PII14 tirregola l-kontrolli preventivi u detettivi tas-sigurtà tal-PII u tal-aċċess.

1.5.10 PII16 tirregola t-taħriġ, is-sensibilizzazzjoni u l-kompetenza dwar il-privatezza.

1.5.11 PII17 tirregola l-informazzjoni dokumentata u l-ġestjoni tal-evidenza.

1.5.12 PII18 tirregola l-monitoraġġ, l-awditjar intern, ir-rieżami mill-maniġment, in-nuqqas ta' konformità, l-azzjoni korrettiva u t-titjib kontinwu.

1.6 Għall-finijiet ta' din il-politika:

1.6.1 "Inċident tal-PII" tfisser avveniment suspettat jew ikkonfermat li affettwa, seta' affettwa, jew jista' raġonevolment jaffettwa l-kunfidenzjalità, l-integrità, id-disponibbiltà, l-ipproċessar legali, jew l-immaniġġjar awtorizzat tal-PII.

1.6.2 "Ksur ta' data personali" tfisser inċident tal-PII ikkonfermat li jinvolvi qerda, telf, alterazzjoni, żvelar, aċċess, indisponibbiltà jew kompromess tal-PII li jkun mhux awtorizzat, illegali, aċċidentali jew mhux intenzjonat.

1.6.3 "Evalwazzjoni tal-ksur" tfisser l-evalwazzjoni dokumentata dwar jekk inċident tal-PII huwiex ksur ta' data personali, liema PII u prinċipali tal-PII huma affettwati, liema riskji jistgħu jinqalgħu, liema notifiki jew komunikazzjonijiet huma meħtieġa, u liema azzjoni rimedjali hija meħtieġa.

1.6.4 "Għarfien" tfisser il-punt meta l-organizzazzjoni jkollha livell raġonevoli ta' ċertezza li seħħ inċident tas-sigurtà jew tal-privatezza u li l-PII ġiet jew setgħet ġiet kompromessa.

1.6.5 "Inċident tal-PII b'impatt għoli" tfisser inċident tal-PII li jinvolvi pproċessar b'riskju għoli, PII ta' kategorija speċjali jew sensittiva ħafna, PII fuq skala kbira, individwi vulnerabbli, klijenti regolati, impatt f'diversi ġurisdizzjonijiet, impatt materjali fuq il-klijent, kompromess ta' aċċess privileġġjat, espożizzjoni pubblika, ransomware, indisponibbiltà tas-servizz, jew impatt operattiv jew reputazzjonali sinifikanti.

1.6.6 "Bidla materjali fl-inċident" tfisser informazzjoni ġdida jew mibdula li taffettwa l-kamp ta' applikazzjoni tal-inċident, is-severità, il-kategoriji tal-PII, l-impatt fuq il-prinċipali tal-PII, id-deċiżjoni ta' notifika, l-impatt fuq il-klijent, il-kawża ewlenija, it-trażżin, l-irkupru, l-azzjoni korrettiva, jew l-obbligi ta' rappurtar estern.

2. Għan

2.1 L-għan ta' din il-politika huwa li tiżgura li l-inċidenti tal-PII u l-ksur ta' data personali jiġu ttrattati b'mod konsistenti, fil-pront, skont il-liġi, b'mod sigur u b'evidenza lesta għall-awditjar.

2.2 Din il-politika tappoġġa r-responsabbiltà billi tirrikjedi li l-inċidenti tal-PII u l-ksur ta' data personali jiġu rreġistrati f'REG10 u marbuta mar-reġistri tal-ipproċessar affettwati, mar-riskji tal-privatezza, mar-relazzjonijiet mal-proċessuri u mas-subproċessuri, mar-reġistri tat-trasferimenti, mal-azzjonijiet korrettivi u mar-reġistri tat-taħriġ fejn dawn jiġu attivati.

2.3 Din il-politika tiżgura li l-obbligi tal-kontrollur, tal-kontrollur konġunt, tal-proċessur u tas-subproċessur jiġu ttrattati permezz ta' regoli distinti ta' applikabbiltà filwaqt li jinżamm mudell integrat wieħed ta' evidenza għall-inċidenti u l-ksur.

3. Objettivi

3.1 L-objettivi ta' din il-politika huma li:

3.1.1 jiġi żgurat li inċidenti suspettati tal-PII jiġu rrappurtati u rreġistrati fil-pront;

3.1.2 jiġi żgurat li inċidenti tal-PII jiġu soġġetti għal trijaġġ u kklassifikati b'kriterji konsistenti;

3.1.3 jiġi żgurat li l-evalwazzjonijiet tal-ksur jikkunsidraw il-PII affettwata, il-prinċipali tal-PII, is-sistemi, l-attivitajiet ta' pproċessar, il-proċessuri, is-subproċessuri, it-trasferimenti, ir-riskji u l-azzjonijiet rimedjali;

3.1.4 jiġi żgurat li d-deċiżjonijiet dwar in-notifika mill-kontrollur u l-komunikazzjoni lill-prinċipali tal-PII jiġu dokumentati;

3.1.5 jiġi żgurat li n-notifiki ta' ksur minn proċessuri u subproċessuri lill-klijenti jew lill-partijiet upstream isiru mingħajr dewmien bla bżonn u skont il-ftehimiet applikabbli;

3.1.6 jiġi żgurat li l-evidenza tinżamm u tiġi protetta waqt l-immaniġġjar tal-inċidenti;

3.1.7 jiġi żgurat li t-trażżin, l-eradikazzjoni, l-irkupru u l-verifika jiġu traċċati permezz ta' REG10;

3.1.8 jiġi żgurat li jiġu evalwati l-attivaturi ta' rappurtar regolati, kuntrattwali, tal-klijenti u settorjali fejn applikabbli;

3.1.9 jiġi żgurat li lessons learned mill-inċidenti jwasslu għal azzjoni korrettiva u titjib kontinwu;

3.1.10 jiġi żgurat li r-reġistri tal-inċidenti u tal-ksur ikunu disponibbli għall-awditjar, għar-rieżami mill-maniġment, għall-assigurazzjoni tal-klijenti u għar-rieżami regolatorju fejn applikabbli.

4. Dikjarazzjonijiet tal-politika

4.1 Tħejjija għall-inċidenti u dħul tar-rapporti

4.1.1 [Both] The Privacy Lead / PIMS Manager MUST iżomm il-kriterji għall-immaniġġjar ta' inċidenti tal-PII u ksur ta' data personali f'REG10 mill-inqas darba fis-sena u wara kwalunkwe bidla materjali fil-kamp ta' applikazzjoni tal-PIMS, fil-kuntest legali, fl-obbligi kuntrattwali jew fl-ipproċessar b'riskju għoli.

4.1.2 [All] The Incident Response Coordinator MUST jirreġistra kull inċident suspettat tal-PII irrappurtat jew skopert f'REG10 fi żmien jum tax-xogħol wieħed minn meta jasal, jew qabel fejn tista' tiġi attivata skadenza applikabbli għan-notifika jew għar-rappurtar lill-klijent.

4.1.3 [Both] The System Owner / Application Owner MUST jippreserva logs tas-sistemi rilevanti, twissijiet, reġistri tal-aċċess, evidenza tal-konfigurazzjoni u evidenza tal-irkupru marbuta ma' REG10 meta inċident suspettat jaffettwa sistema jew applikazzjoni li tipproċessa PII.

4.1.4 [Both] The Information Security Lead MUST itemm it-trijaġġ tekniku inizjali ta' kwalunkwe avveniment tas-sigurtà li jinvolvi PII fi żmien 24 siegħa mill-iskoperta u jirreġistra s-severità inizjali, l-assi affettwati u l-istatus tat-trażżin f'REG10.

4.2 Klassifikazzjoni u evalwazzjoni tal-ksur

4.2.1 [Both] The Incident Response Coordinator MUST jikklassifika kull entrata f'REG10 bħala avveniment mhux tal-PII, inċident suspettat tal-PII, inċident ikkonfermat tal-PII, jew ksur ikkonfermat ta' data personali fi żmien 24 siegħa mid-dħul tar-rapport, jew jaġġorna r-reġistru ta' REG10 bir-raġuni għalfejn il-klassifikazzjoni għadha pendenti.

4.2.2 [Both] The Privacy Lead / PIMS Manager MUST jidentifika l-attività ta' pproċessar affettwata, il-kategoriji tal-PII, il-kategoriji tal-prinċipali tal-PII, is-sistemi, il-proċessuri, is-subproċessuri, il-postijiet tat-trasferiment u r-riskji tal-privatezza f'REG02, REG04, REG08, REG09 u REG10 qabel ma tiġi ffinalizzata d-deċiżjoni tan-notifika tal-ksur.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST jevalwa r-riskju għall-prinċipali tal-PII affettwati għal kull ksur ikkonfermat jew raġonevolment suspettat ta' data personali u jirreġistra r-rakkomandazzjoni tan-notifika, ir-raġunament dwar ir-riskju u l-parir f'REG10 qabel ma tittieħed id-deċiżjoni tan-notifika esterna.

4.2.4 [Processor] The Privacy Lead / PIMS Manager MUST jidentifika l-kontrollur jew il-klijent affettwat u r-rekwiżiti kuntrattwali applikabbli għan-notifika hekk kif l-organizzazzjoni ssir taf b'ksur ta' data personali li jaffettwa PII tal-klijent, u MUST jirreġistra l-eżitu f'REG08 u REG10.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST jivverifika r-responsabbiltà miftiehma għall-ksur, ir-responsabbiltà ewlenija għall-komunikazzjoni u l-arranġament ta' koordinazzjoni qabel kwalunkwe notifika jew komunikazzjoni esterna minn kontrollur konġunt, u MUST jirreġistra d-deċiżjoni f'REG08 u REG10.

4.2.6 [Conditional] The Privacy Lead / PIMS Manager MUST jevalwa l-attivaturi applikabbli ta' rappurtar legali, settorjali, tas-settur finanzjarju, taċ-ċibersigurtà, kuntrattwali, tal-klijent u tar-riċevitur tas-servizz għal kull inċident tal-PII b'impatt għoli u jirreġistra l-eżitu tal-applikabbiltà f'REG01, REG08 u REG10.

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

9. Eċċezzjonijiet

9.1.1 [Both] The Privacy Lead / PIMS Manager MUST jirreġistra kwalunkwe eċċezzjoni għal din il-politika f'REG12 qabel l-implimentazzjoni, jew fi żmien 24 siegħa wara azzjoni ta' emerġenza fejn approvazzjoni minn qabel ma kinitx fattibbli.

9.1.2 [Both] Top Management MUST japprova kwalunkwe eċċezzjoni li taffettwa materjalment iż-żmien tan-notifika tal-ksur, il-komunikazzjoni pubblika, l-impenn mal-klijent, il-preservazzjoni tal-evidenza jew ir-riskju għall-prinċipali tal-PII qabel ma jingħalaq l-inċident, b'evidenza tal-approvazzjoni miżmuma f'REG10 u REG12.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST jiddokumenta parir għal kwalunkwe notifika mdewma, deċiżjoni ta' nuqqas ta' notifika, jew approċċ eċċezzjonali ta' komunikazzjoni qabel l-għeluq tal-inċident, bil-parir miżmum f'REG10.

9.1.4 [Both] The Vendor / Procurement Owner MUST jirreġistra eċċezzjonijiet immexxija minn fornitur, proċessur, subproċessur jew klijent li jaffettwaw ir-rispons għall-inċident f'REG08 u REG12 fi żmien ħamest ijiem tax-xogħol minn meta tiġi identifikata l-eċċezzjoni.

10. Applikazzjoni

10.1.1 [All] The Process Owner / Business Owner MUST jeskala nuqqas ta' rappurtar ta' inċident suspettat tal-PII, preservazzjoni tal-evidenza, segwitu ta' azzjonijiet assenjati jew kooperazzjoni mal-evalwazzjoni tal-ksur lil The Privacy Lead / PIMS Manager fi żmien żewġ ijiem tax-xogħol mill-iskoperta, bl-evidenza miżmuma f'REG12.

10.1.2 [Both] The Privacy Lead / PIMS Manager MUST jirreġistra nuqqas ta' konformità f'REG12 meta ksur ta' din il-politika jaffettwa d-dħul tar-rapporti tal-inċidenti, it-trijaġġ, it-trażżin, in-notifika, l-integrità tal-evidenza, il-komunikazzjoni jew l-azzjoni korrettiva.

10.1.3 [Both] The Vendor / Procurement Owner MUST jibda rimedjazzjoni tal-fornitur jew tal-proċessur permezz ta' REG08 u REG12 fi żmien ħamest ijiem tax-xogħol meta proċessur, subproċessur, fornitur jew parti terza oħra tonqos milli tissodisfa l-obbligi miftiehma dwar inċidenti jew ksur.

10.1.4 [Both] Top Management MUST jirrieżamina nuqqasijiet ta' konformità materjali jew rikorrenti fil-ġestjoni tal-inċidenti fir-rieżami mill-maniġment skedat li jmiss, bid-deċiżjonijiet u l-azzjonijiet meħtieġa miżmuma f'REG12.

11. Rieżami u manutenzjoni

11.1.1 [Both] The Privacy Lead / PIMS Manager MUST jirrieżamina din il-politika mill-inqas darba fis-sena u jirreġistra l-eżitu tar-rieżami, il-bidliet meħtieġa u l-istatus tal-approvazzjoni f'REG12.

11.1.2 [Both] The Incident Response Coordinator MUST jattiva rieżami ta' din il-politika wara l-inċident fi żmien 30 jum kalendarju wara l-għeluq ta' kwalunkwe inċident tal-PII b'impatt għoli jew ksur ikkonfermat ta' data personali, b'evidenza tar-rieżami miżmuma f'REG10 u REG12.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUST jirrieżamina din il-politika fi żmien 30 jum kalendarju minn meta jsir jaf b'bidla materjali fir-rekwiżiti applikabbli ta' rappurtar ta' inċidenti legali, settorjali, tal-klijent, kuntrattwali, tal-proċessur, tas-subproċessur jew relatati mat-trasferiment, b'evidenza tar-rieżami miżmuma f'REG01, REG08, REG09 u REG12.

11.1.4 [Both] The Internal Audit / Compliance Reviewer MUST jirrieżamina l-implimentazzjoni ta' din il-politika mill-inqas darba fis-sena permezz tal-programm ta' awditjar intern tal-PIMS, bis-sejbiet tal-awditjar u l-azzjonijiet korrettivi miżmuma f'REG12.

11.1.5 [Both] Top Management MUST jirrieżamina x-xejriet tal-inċidenti, ksur sinifikanti, prestazzjoni tan-notifiki, azzjonijiet korrettivi skaduti u l-effettività tal-politika matul ir-rieżami skedat mill-maniġment, bl-outputs miżmuma f'REG12.

12. Politiki relatati

12.1 Din il-politika għandha tinqara flimkien ma':

12.2 PII01 - Politika tas-Sistema ta' Ġestjoni tal-Informazzjoni dwar il-Privatezza

12.3 PII02 - Politika dwar ir-Rwoli, ir-Responsabbiltajiet u r-Responsabbiltà fil-Privatezza

12.4 PII03 - Politika dwar l-Inventarju tal-Ipproċessar tal-PII u l-Bażi Legali

12.5 PII04 - Politika dwar l-Avviż ta' Privatezza u t-Trasparenza

12.6 PII06 - Politika għall-Ġestjoni tad-Drittijiet tal-Prinċipali tal-PII

12.7 PII07 - Politika dwar il-Valutazzjoni tar-Riskju tal-Privatezza u d-DPIA

12.8 PII08 - Politika dwar il-Privatezza mid-Disinn u b'Mod Predefinit

12.9 PII10 - Politika dwar iż-Żamma, it-Tħassir u r-Rimi tal-PII

12.10 PII12 - Politika dwar il-Ġestjoni tal-Privatezza ta' Proċessuri, Subproċessuri u Partijiet Terzi

12.11 PII13 - Politika dwar it-Trasferiment Internazzjonali tal-PII

12.12 PII14 - Politika dwar is-Sigurtà tal-PII u l-Kontroll tal-Aċċess

12.13 PII16 - Politika dwar it-Taħriġ, is-Sensibilizzazzjoni u l-Kompetenza fil-Privatezza

12.14 PII17 - Politika dwar l-Informazzjoni Dokumentata u l-Ġestjoni tal-Evidenza tal-PIMS

12.15 PII18 - Politika dwar il-Monitoraġġ, l-Awditjar u t-Titjib tal-PIMS

13. Standards u oqfsa ta' referenza

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].