					Daħħal hawn l-isem tal-entità ġuridika rreġistrata						
Numru tad-dokument: PII15-FS					Titlu tad-dokument: **Politika għall-Ġestjoni tal-Inċidenti u l-Ksur tal-PII fis-Settur Finanzjarju**						
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**

Avviż legali (drittijiet tal-awtur u restrizzjonijiet fuq l-użu)
(C) 2025 Clarysec LLC. All rights reserved.

Dan id-dokument huwa proprjetà intellettwali ta' Clarysec LLC. L-ebda parti minn dan id-dokument ma tista' tiġi kkupjata, użata mill-ġdid, distribwita jew modifikata għal skopijiet kummerċjali jew ta' implimentazzjoni mingħajr awtorizzazzjoni espliċita minn qabel bil-miktub.
L-użu mhux awtorizzat huwa strettament ipprojbit u jista' jwassal għal azzjoni legali.
Għal-liċenzjar, ikkuntattja: info@clarysec.com

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 tal-inċidenti
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 fl-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	Appoġġ għall-ftehim mal-klijent tal-proċessur u 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-inċidenti bejn kontrolluri konġunti
GDPR	Article 28	Both	Supporting	Assistenza mill-proċessur u obbligi kuntrattwali tal-proċessur

GDPR	Article 32	Both	Supporting	Sigurtà tal-ipproċessar u kapaċità ta' skoperta tal-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
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Proċess ta' ġestjoni ta' inċidenti relatati mal-ICT għal entitajiet finanzjarji fil-kamp ta' applikazzjoni
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Kriterji ta' klassifikazzjoni għal inċidenti relatati mal-ICT u theddid ċibernetiku sinifikanti
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Rappurtar ta' inċidenti maġġuri relatati mal-ICT u notifika ta' theddid ċibernetiku sinifikanti
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Kontenut tar-rappurtar, limiti ta' żmien, mudelli u proċeduri
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Rappurtar ta' inċidenti sinifikanti fejn applikabbli
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Prinċipji tas-sigurtà tal-informazzjoni u tal-konformità tal-privatezza

ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Responsabbiltajiet tar-rispons għall-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 ta' 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 għall-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 għal notifika u reġistru tal-ksur minn proċessur tal-cloud pubbliku

1. Kamp ta' applikazzjoni

1.1 Din il-politika tiddefinixxi r-rekwiżiti għall-identifikazzjoni, ir-rappurtar, it-trijaġġ, il-klassifikazzjoni, l-evalwazzjoni, it-trażżin, in-notifika, id-dokumentazzjoni, l-għeluq u t-titjib minn inċidenti tal-PII u ksur ta' data personali fil-kampijiet ta' applikazzjoni tal-PIMS tas-settur finanzjarju.

1.2 **Avviż ta' implimentazzjoni:** Din il-politika hija varjant sostitut ta' PII15 għas-settur finanzjarju. Ma għandhiex tiġi implimentata fl-istess ħin ma' PII15 għall-istess kamp ta' applikazzjoni tal-PIMS, unità tan-negozju, prodott, ambjent tal-klijent, servizz regolat jew limitu tal-evidenza. L-organizzazzjonijiet għandhom jagħżlu jew PII15 jew PII15-FS għall-istess kamp ta' applikazzjoni sabiex jevitaw obbligi duplikati ta' ġestjoni tal-inċidenti, reġistri duplikati u xogħol duplikat fuq evidenza tal-awditjar.

1.3 Din il-politika tapplika għal:

1.3.1 l-organizzazzjoni li taġixxi bħala kontrollur tal-PII f'kuntest tas-settur finanzjarju;

1.3.2 l-organizzazzjoni li taġixxi bħala kontrollur konġunt fejn tkun meħtieġa koordinazzjoni tar-responsabbiltà għal inċident jew ksur;

1.3.3 l-organizzazzjoni li taġixxi bħala proċessur tal-PII għal klijenti tas-settur finanzjarju;

1.3.4 l-organizzazzjoni li taġixxi bħala subproċessur għal klijenti tas-settur finanzjarju jew proċessuri upstream;

1.3.5 sistemi, applikazzjonijiet, servizzi, proċessi, forniturі, proċessuri, subproċessuri u partijiet terzi li jipproċessaw, jaħżnu, jittrażmettu, jappoġġaw, jaċċessaw jew b'xi mod ieħor jaffettwaw PII fil-kamp ta' applikazzjoni tal-PIMS tas-settur finanzjarju.

1.4 Din il-politika tuża REG10 - Reġistru tal-Inċidenti u l-Ksur tal-PII bħala l-oġġett ewlieni ta' evidenza għall-ġestjoni tal-inċidenti tal-PII u l-ksur ta' data personali fis-settur finanzjarju.

1.5 Din il-politika tuża oġġetti ta' evidenza ta' appoġġ kif ġej:

1.5.1 REG01 għall-kamp ta' applikazzjoni tal-PIMS, u għall-kuntest applikabbli tal-partijiet interessati, settorjali, tal-klijent, kuntrattwali u tar-rappurtar.

1.5.2 REG02 għall-attivitajiet ta' pproċessar affettwati, kategoriji tal-PII, kategoriji ta' prinċipali tal-PII, għanijiet, sistemi u servizzi.

1.5.3 REG03 għad-Dikjarazzjoni ta' Applikabbiltà u għall-aġġornamenti tal-applikabbiltà tal-kontrolli, inkluż is-sostituzzjoni ta' PII15 minn PII15-FS għall-istess kamp ta' applikazzjoni.

1.5.4 REG04 għar-riskju tal-privatezza, DPIA, riskju residwu u rabta mat-trattament tar-riskju.

1.5.5 REG08 għall-evidenza tal-interfaċċa tal-inċidenti mal-proċessuri, is-subproċessuri, il-klijenti, il-forniturі u l-partijiet terzi.

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

1.5.7 REG11 għall-evidenza ta' taħriġ, sensibilizzazzjoni u kompetenza fir-rispons għall-inċidenti.

1.5.8 REG12 għall-evidenza tal-awditjar, in-nuqqas ta' konformità, l-azzjoni korrettiva, ir-rieżami tal-ġestjoni u t-titjib.

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

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

1.6.2 PII04 tirregola l-avviż ta' privatezza u l-kontrolli tat-trasparenza barra l-komunikazzjonijiet speċifiċi għall-ksur.

1.6.3 PII06 tirregola t-talbiet tad-drittijiet tal-prinċipal tal-PII li jinqalgħu qabel, waqt jew wara inċident.

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

1.6.5 PII08 tirregola l-kontrolli tal-privatezza mid-disinn u l-privatezza b'mod predefinit.

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

1.6.7 PII12 tirregola l-kontrolli tar-relazzjonijiet ta' privatezza mal-proċessuri, is-subproċessuri, il-fornituri u l-partijiet terzi.

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

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

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

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

1.6.12 PII18 tirregola l-monitoraġġ, l-awditjar intern, ir-rieżami tal-ġestjoni, in-nuqqas ta' konformità, l-azzjoni korrettiva u t-titjib kontinwu.

1.6.13 PII23 tirregola l-kontrolli tal-proċessuri tal-PII fil-cloud fejn l-obbligi tal-proċessuri cloud ikunu fil-kamp ta' applikazzjoni.

1.7 Għall-finijiet ta' din il-politika:

1.7.1 "PII incident" tfisser avveniment suspettat jew ikkonfermat li affettwa, seta' affettwa jew jista' b'mod raġonevoli jaffettwa l-kunfidenzjalità, l-integrità, id-disponibbiltà, l-ipproċessar legali jew l-immaniġġjar awtorizzat tal-PII.

1.7.2 "PII breach" tfisser inċident tal-PII ikkonfermat li jinvolvi qerda, telf, alterazzjoni, żvelar, aċċess, nuqqas ta' disponibbiltà jew kompromess tal-PII mhux awtorizzat, illegali, aċċidentali jew mhux intenzjonat.

1.7.3 "Financial-sector PII incident" tfisser inċident tal-PII li jaffettwa, jista' jaffettwa jew huwa raġonevolment marbut ma' servizzi finanzjarji regolati, klijenti tas-settur finanzjarju, kontropartijiet finanzjarji, tranżazzjonijiet finanzjarji, operazzjonijiet finanzjarji jew ipproċessar tal-PII fis-settur finanzjarju.

1.7.4 "Major financial-sector incident" tfisser inċident tal-PII fis-settur finanzjarju jew inċident relatat mal-ICT li jissodisfa kriterji dokumentati ta' materjalità jew rappurtar f'REG10.

1.7.5 "Significant cyber threat" tfisser theddida ċibernetika rreġistrata f'REG10 li tista' taffettwa b'mod materjali s-servizzi tas-settur finanzjarju, l-ipproċessar tal-PII, il-klijenti, il-kontropartijiet jew l-operazzjonijiet fil-kamp ta' applikazzjoni.

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

1.7.7 "Awareness" tfisser il-punt li fih l-organizzazzjoni jkollha grad raġonevoli ta' ċertezza li seħħ inċident ta' sigurtà jew privatezza u li l-PII ġiet jew setgħet ġiet kompromessa.

1.7.8 "High-impact financial-sector PII incident" 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, tfixkil materjali tas-servizz, kontropartijiet finanzjarji, tranżazzjonijiet finanzjarji, impatt f'diversi ġurisdizzjonijiet, kompromess ta' aċċess privileġġjat, espożizzjoni pubblika, ransomware, nuqqas ta' disponibbiltà tas-servizz jew impatt operattiv, fuq il-klijent, finanzjarju jew reputazzjonali sinifikanti.

1.7.9 "Material incident change" tfisser informazzjoni ġdida jew mibdula li taffettwa l-kamp tal-inċident, is-severità, il-kategoriji tal-PII, l-impatt fuq il-prinċipali tal-PII, l-impatt fuq is-servizz, il-klassifikazzjoni tas-settur finanzjarju, id-deċiżjoni dwar in-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 f'kuntesti tas-settur finanzjarju jiġu mmaniġġjati b'mod konsistenti, fil-pront, legalment, b'mod sigur u b'evidenza lesta għall-awditjar.

2.2 Din il-politika tappoġġa r-responsabbiltà billi teħtieġ li l-inċidenti tal-PII u l-ksur ta' data personali fis-settur finanzjarju jiġu rreġistrati f'REG10 u marbuta ma' reġistri tal-ipproċessar affettwati, riskji tal-privatezza, relazzjonijiet ma' proċessuri u subproċessuri, reġistri tat-trasferimenti, azzjonijiet korrettivi, reġistri tat-taħriġ, deċiżjonijiet ta' rappurtar tas-settur finanzjarju u evidenza tar-rieżami tal-ġestjoni fejn jiġu skattati.

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

3. Objettivi

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

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

3.1.2 jiġi żgurat li inċidenti tal-PII fis-settur finanzjarju jgħaddu minn trijaġġ u jiġu kklassifikati bl-użu ta' kriterji konsistenti ta' privatezza, sigurtà, operazzjonijiet u settur;

3.1.3 jiġi żgurat li l-evalwazzjonijiet tal-ksur jikkunsidraw il-PII affettwata, il-prinċipali tal-PII, is-sistemi, is-servizzi, l-attivitajiet ta' pproċessar, il-proċessuri, is-subproċessuri, it-trasferimenti, ir-riskji, il-klijenti, il-kontropartijiet 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 tal-ksur mill-proċessuri u s-subproċessuri lill-klijenti jew lill-partijiet upstream isiru mingħajr dewmien żejjed u skont il-ftehimiet applikabbli;

3.1.6 jiġi żgurat li l-iskattaturi tar-rappurtar tas-settur finanzjarju jiġu evalwati, dokumentati u segwiti fejn applikabbli;

3.1.7 jiġi żgurat li l-evidenza tiġi ppreservata u protetta waqt l-immaniġġjar tal-inċident;

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

3.1.9 jiġi żgurat li theddid ċibernetiku sinifikanti u inċidenti maġġuri fis-settur finanzjarju jiġu indirizzati lejn flussi tax-xogħol xierqa għad-deċiżjoni u r-rappurtar;

3.1.10 jiġi żgurat li l-lessons learned mill-inċidenti jwasslu għal azzjoni korrettiva, taħriġ, titjib tal-kontrolli u rieżami tal-ġestjoni;

3.1.11 jiġi żgurat li r-reġistri tal-inċidenti u l-ksur ikunu disponibbli għall-awditjar, ir-rieżami tal-ġestjoni, l-assigurazzjoni tal-klijenti u r-rieżami regolatorju fejn applikabbli;

3.1.12 jiġi żgurat li PII15-FS tissostitwixxi PII15 għall-istess kamp ta' applikazzjoni tas-settur finanzjarju u ma tidduplikax ix-xogħol tal-evidenza ta' PII15.

4. Dikjarazzjonijiet tal-politika

4.1 Attivazzjoni tal-varjant, tħejjija u akkoljenza

4.1.1 [Conditional] The Privacy Lead / PIMS Manager GĦANDU jiddokumenta l-attivazzjoni ta' PII15-FS f'REG01 u REG03 qabel ma din il-politika tintuża għal kamp ta' applikazzjoni tal-PIMS fis-settur finanzjarju.

4.1.2 [Conditional] The Privacy Lead / PIMS Manager GĦANDU jiddokumenta f'REG03 u REG12 li PII15 mhijiex implimentata fl-istess ħin għall-istess kamp ta' applikazzjoni tal-PIMS fis-settur finanzjarju qabel ma PII15-FS tiġi approvata.

4.1.3 [All] The Incident Response Coordinator GĦANDU jirreġistra kull inċident suspettat tal-PII fis-settur finanzjarju rrappurtat jew skopert f'REG10 fi żmien jum wieħed tax-xogħol minn meta jiġi riċevut, jew qabel fejn tista' tiġi skattata skadenza applikabbli ta' notifika, ta' klijent jew ta' rappurtar.

4.1.4 [Conditional] The Privacy Lead / PIMS Manager GĦANDU jżomm kriterji għall-immaniġġjar tal-inċidenti tal-PII u l-ksur ta' data personali fis-settur finanzjarju f'REG10 mill-inqas kull sena u wara kwalunkwe bidla materjali fil-kamp ta' applikazzjoni tal-PIMS, fil-kuntest legali, fl-obbligi tal-klijenti, fl-obbligi kuntrattwali, fil-kuntest tar-rappurtar settorjali jew fl-ipproċessar b'riskju għoli.

4.1.5 [Both] The Information Security Lead GĦANDU jikkonferma r-rekwiżiti għall-preservazzjoni tal-evidenza tal-inċident f'REG10 fi żmien 24 siegħa wara li inċident suspettat jaffettwa sistema, servizz jew applikazzjoni li tipproċessa PII.

4.1.6 [Conditional] The Vendor / Procurement Owner GĦANDU jżomm ir-rekwiżiti ta' kuntatt u rotta tal-evidenza għal inċidenti ma' partijiet terzi tas-settur finanzjarju f'REG08 qabel l-onboarding u mill-inqas kull sena għall-proċessuri, is-subproċessuri, il-forniturі u l-forniturі esternalizzati tar-rappurtar fil-kamp ta' applikazzjoni.

4.2 Klassifikazzjoni u evalwazzjoni tal-ksur

4.2.1 [All] The Incident Response Coordinator GĦANDU jikklassifika kull entrata f'REG10 fi żmien 24 siegħa mill-akkoljenza bħala avveniment mhux tal-PII, inċident suspettat tal-PII, inċident ikkonfermat tal-PII, ksur ikkonfermat ta' data personali, inċident tal-PII fis-settur finanzjarju, inċident maġġuri fis-settur finanzjarju, theddida ċibernetika sinifikanti jew entrata pendenti għall-klassifikazzjoni.

4.2.2 [Conditional] The Information Security Lead GĦANDU jevalwa s-servizzi, il-klijenti, il-kontropartijiet, it-tranżazzjonijiet, il-ħin ta' waqfien tas-servizz, it-tixrid ġeografiku, it-telf tad-data, il-kritiċità tas-servizz u l-impatt ekonomiku affettwati f'REG10 meta inċident tal-PII jista' jaffettwa servizzi jew operazzjonijiet tas-settur finanzjarju.

4.2.3 [Both] The Privacy Lead / PIMS Manager GĦANDU 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 d-deċiżjoni dwar in-notifika tal-ksur tiġi ffinalizzata.

4.2.4 [Controller] The Data Protection Officer / Privacy Advisor GĦANDU jevalwa r-riskju għall-prinċipali tal-PII affettwati għal kull ksur ta' data personali kkonfermat jew suspettat b'mod raġonevoli u jirreġistra r-rakkomandazzjoni dwar in-notifika, ir-raġunament tar-riskju u l-parir f'REG10 qabel ma tittieħed id-deċiżjoni dwar in-notifika esterna.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager GĦANDU jirreġistra l-allokazzjoni tar-responsabbiltà għall-inċident bejn kontrolluri konġunti f'REG08 u REG10 fi żmien 24 siegħa wara li jidentifika responsabbiltà kondiviża għal ksur ta' data personali suspettat jew ikkonfermat.

4.2.6 [Processor] The Privacy Lead / PIMS Manager GĦANDU jevalwa l-istruzzjonijiet tal-klijent, l-obbligi kuntrattwali ta' notifika u l-obbligi ta' kooperazzjoni f'REG08 u REG10 fi żmien 24 siegħa wara li ksur ta' data personali suspettat jew ikkonfermat jaffettwa pproċessar imwettaq bħala proċessur.

4.2.7 [Subprocessor] The Vendor / Procurement Owner GĦANDU jidentifika l-katina ta' notifika upstream u r-rotta meħtieġa tal-evidenza f'REG08 u REG10 fi żmien 24 siegħa wara li inċident tal-PII suspettat jew ikkonfermat jaffettwa pproċessar imwettaq bħala subproċessur.

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

9.1.2 [Conditional] Top Management GĦANDU japprova kwalunkwe eċċezzjoni li taffettwa b'mod materjali ż-żmien tan-notifika tal-ksur, iż-żmien tar-rappurtar tas-settur finanzjarju, il-komunikazzjoni pubblika, l-impenn mal-klijent, il-preservazzjoni tal-evidenza jew ir-riskju għall-prinċipali tal-PII qabel ma l-inċident jingħalaq, bl-evidenza tal-approvazzjoni miżmuma f'REG10 u REG12.

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

9.1.4 [Both] The Vendor / Procurement Owner GĦANDU jirreġistra eċċezzjonijiet ta' fornitur, proċessur, subproċessur, klijent jew fornitur esternalizzat li jaffettwaw ir-rispons għall-inċidenti tas-settur finanzjarju f'REG08 u REG12 fi żmien ħamest ijiem tax-xogħol wara li jidentifika l-eċċezzjoni.

9.1.5 [All] The Privacy Lead / PIMS Manager GĦANDU jirrieżamina eċċezzjonijiet miftuħa għal din il-politika mill-inqas kull xahar sal-għeluq, bl-istatus tar-rieżami miżmum f'REG12.

10. Applikazzjoni

10.1.1 [All] The Process Owner / Business Owner GĦANDU jeskala n-nuqqas li jiġi rrappurtat inċident suspettat tal-PII fis-settur finanzjarju, li tiġi ppreservata l-evidenza, li jiġu segwiti azzjonijiet assenjati jew li ssir kooperazzjoni fl-evalwazzjoni tal-ksur lil The Privacy Lead / PIMS Manager fi żmien żewġ ijiem tax-xogħol wara l-iskoperta, bl-evidenza miżmuma f'REG12.

10.1.2 [Both] The Incident Response Coordinator GĦANDU jeskala rappurtar tard, klassifikazzjoni mitlufa, evidenza nieqsa, eskalazzjoni mitlufa jew azzjoni ta' trażżin li qabżet l-iskadenza lil The Privacy Lead / PIMS Manager fi żmien jum wieħed tax-xogħol wara li jidentifika l-kwistjoni, bl-evidenza miżmuma f'REG10 u REG12.

10.1.3 [Both] The Privacy Lead / PIMS Manager GĦANDU jirreġistra nuqqas ta' konformità f'REG12 meta ksur ta' din il-politika jaffettwa l-akkoljenza, it-trijaġġ, it-trażżin, in-notifika, ir-rappurtar, l-integrità tal-evidenza, il-komunikazzjoni jew l-azzjoni korrettiva tal-inċident.

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

10.1.5 [Conditional] Top Management GĦANDU jirrieżamina nuqqasijiet ta' konformità materjali jew rikorrenti ta' PII15-FS fir-rieżami skedat li jmiss tal-ġestjoni, bid-deċiżjonijiet u l-azzjonijiet meħtieġa miżmuma f'REG12.

10.1.6 [All] The Privacy Lead / PIMS Manager GĦANDU jiskatta taħriġ rimedjali f'REG11 fi żmien 30 jum kalendarju meta nuqqas ta' konformità mal-politika jinvolvi sensibilizzazzjoni tar-rwol, rappurtar tard, falliment fl-eskalazzjoni, falliment fl-immaniġġjar tal-evidenza jew falliment fil-komunikazzjoni.

11. Rieżami u manutenzjoni

11.1.1 [Conditional] The Privacy Lead / PIMS Manager GĦANDU jirrieżamina din il-politika mill-inqas kull sena u jirreġistra r-riżultat tar-rieżami, il-bidliet meħtieġa u l-istatus tal-approvazzjoni f'REG12.

11.1.2 [Conditional] The Incident Response Coordinator GĦANDU jiskatta rieżami wara l-inċident ta' din il-politika fi żmien 30 jum kalendarju wara l-għeluq ta' kwalunkwe inċident tal-PII b'impatt għoli fis-settur finanzjarju, ksur ikkonfermat ta' data personali, inċident maġġuri fis-settur finanzjarju jew theddida ċibernetika sinifikanti, bl-evidenza tar-rieżami miżmuma f'REG10 u REG12.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager GĦANDU jirrieżamina din il-politika fi żmien 30 jum kalendarju wara li jsir jaf b'bidla materjali fir-rekwiżiti legali, settorjali, tal-klijent, kuntrattwali, tal-proċessur, tas-subproċessur, tal-mudell tar-rappurtar, tal-iskeda tar-rappurtar jew relatati mat-trasferimenti għar-rappurtar tal-inċidenti, bl-evidenza tar-rieżami miżmuma f'REG01, REG08, REG09 u REG12.

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

11.1.5 [Conditional] Top Management GĦANDU jirrieżamina x-xejriet tal-inċidenti, ksur sinifikanti, il-prestazzjoni tar-rappurtar, azzjonijiet korrettivi li qabżu l-iskadenza u l-effettività tal-politika waqt ir-rieżami skedat tal-ġestjoni, bl-outputs miżmuma f'REG12.

11.1.6 [Conditional] The Privacy Lead / PIMS Manager GĦANDU jirrieżamina r-relazzjoni ta' sostituzzjoni bejn PII15-FS u PII15 mill-inqas kull sena u wara kwalunkwe bidla fil-kamp ta' applikazzjoni tal-PIMS biex jivverifika li ż-żewġ politiki mhumiex implimentati għall-istess kamp ta' applikazzjoni tas-settur finanzjarju, bl-evidenza tar-rieżami miżmuma f'REG03 u REG12.

12. Politiki relatati

12.1 Din il-politika għandha tinqara flimkien ma':

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

12.1.2 PII02 - Politika dwar ir-Rwoli, ir-Responsabbiltajiet u r-Responsabbiltà tal-Privatezza

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

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

12.1.5 PII06 - Politika dwar il-Ġestjoni tad-Drittijiet tal-Prinċipali tal-PII

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

12.1.7 PII08 - Politika dwar il-Privatezza mid-Disinn u b'mod Predefinit

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

12.1.9 PII12 - Politika dwar il-Ġestjoni tal-Privatezza tal-Proċessuri, is-Subproċessuri u l-Partijiet Terzi

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

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

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

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

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

12.1.15 PII23 - Politika dwar il-Proċessur tal-PII fil-Cloud, fejn l-obbligi tal-proċessur cloud fis-settur finanzjarju jkunu fil-kamp ta' applikazzjoni

12.2 PII15 - Politika dwar il-Ġestjoni tal-Inċidenti u l-Ksur tal-PII hija l-politika bażi għall-inċidenti u l-ksur. PII15-FS hija varjant sostitut ta' PII15 għas-settur finanzjarju. PII15 u PII15-FS ma għandhomx jiġu implimentati fl-istess ħin għall-istess kamp ta' applikazzjoni tal-PIMS, unità tan-negozju, prodott, ambjent tal-klijent, servizz regolat jew limitu tal-evidenza.

13. Standards u oqfsa ta' referenza

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 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; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 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 [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].