					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII01					Titolo del documento: **Politica del Sistema di gestione delle informazioni sulla privacy**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a standard e normative applicabili

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Contesto e determinazione del ruolo PIMS
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Parti interessate e requisiti
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	Ambito di applicazione del PIMS
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Istituzione e miglioramento del PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Leadership e impegno
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Politica privacy
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Ruoli e autorità
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Rischi e opportunità
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Valutazione del rischio privacy
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Trattamento del rischio privacy e SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Obiettivi privacy
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Modifiche pianificate del PIMS
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Risorse
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competenza
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Consapevolezza
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Comunicazioni
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informazioni documentate

ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Pianificazione operativa e controllo
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Valutazione operativa del rischio privacy
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Trattamento operativo del rischio privacy
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitoraggio e valutazione
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Audit interno
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Riesame della direzione
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Miglioramento continuo
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Non conformità e azione correttiva
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Registrazioni di governance del titolare del trattamento
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Accordo e finalità del responsabile del trattamento
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Collegamento alla politica di sicurezza delle PII
GDPR	Article 5(2)	Controller	Supporting	Evidenze di accountability
GDPR	Article 24	Controller	Supporting	Misure e politica del titolare del trattamento
GDPR	Article 26	Joint Controller	Supporting	Accordi di contitolarità del trattamento
GDPR	Article 28	Both	Supporting	Governance dei responsabili del trattamento
GDPR	Article 30	Both	Supporting	Registrazioni dei trattamenti

GDPR	Article 32	Both	Supporting	Sicurezza del trattamento
GDPR	Article 35	Controller	Supporting	Governance della DPIA
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Controlli e principi privacy
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Processo PIA e preparazione
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	Programma e politica di protezione delle PII
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integrazione del rischio privacy organizzativo

1. Ambito di applicazione

1.1 La presente politica istituisce il Sistema di gestione delle informazioni sulla privacy dell'organizzazione per il trattamento delle PII nei contesti di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile.

1.2 La presente politica si applica a:

1.2.1 ambito di applicazione, contesto, parti interessate e confini organizzativi del PIMS;

1.2.2 determinazione del ruolo PIMS per le attività di trattamento delle PII;

1.2.3 politica privacy, obiettivi privacy, valutazione del rischio privacy, trattamento del rischio privacy e Dichiarazione di Applicabilità del PIMS;

1.2.4 governance, monitoraggio, audit interno, riesame della direzione, non conformità, azione correttiva e miglioramento continuo del PIMS;

1.2.5 informazioni documentate ed evidenze necessarie per dimostrare la conformità del PIMS e l'accountability.

1.3 Ai fini della presente politica, per modifica significativa si intende qualsiasi modifica che incida sull'ambito di applicazione del PIMS, sulle finalità del trattamento delle PII, sulle categorie di PII, sulle categorie di interessati, sui luoghi di trattamento, sull'attribuzione del ruolo di titolare del trattamento o di responsabile del trattamento, sull'architettura dei sistemi, sugli accordi con fornitori o sub-responsabili, sul profilo di rischio privacy, sugli obblighi legali o contrattuali applicabili, o sull'ambito di certificazione.

2. Finalità

2.1 La presente politica definisce i requisiti obbligatori di governance per istituire, attuare, mantenere, monitorare e migliorare continuamente il PIMS.

2.2 La finalità della presente politica è garantire che l'organizzazione possa dimostrare una gestione del trattamento delle PII responsabile, basata sul rischio e fondata su evidenze in tutti i ruoli PIMS applicabili.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 definire l'ambito di applicazione, il contesto, i confini e l'applicabilità dei ruoli del PIMS;

3.1.2 attribuire la responsabilità di governance del PIMS utilizzando i ruoli PIMS canonici;

3.1.3 stabilire obiettivi privacy e aspettative misurabili di prestazione del PIMS;

3.1.4 mantenere una Dichiarazione di Applicabilità del PIMS per i controlli selezionati ed esclusi;

3.1.5 integrare la valutazione del rischio privacy, il trattamento del rischio privacy e la governance della DPIA nell'operatività del PIMS;

3.1.6 garantire che gli obblighi di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile siano identificati prima dell'avvio del trattamento;

3.1.7 mantenere evidenze pronte per l'audit a supporto della preparazione alla certificazione e del miglioramento continuo;

3.1.8 evitare ruoli, registri, moduli e controlli operativi duplicati non necessari.

4. Dichiarazioni della politica

4.1 Istituzione, contesto e ambito di applicazione del PIMS

4.1.1 [Both] Top Management deve approvare l'ambito di applicazione del PIMS in REG01 prima dell'attuazione iniziale del PIMS ed entro 30 giorni da qualsiasi modifica significativa.

4.1.2 [Both] Privacy Lead / PIMS Manager deve documentare in REG01 le questioni esterne e interne relative al contesto privacy con cadenza annuale ed entro 30 giorni da qualsiasi modifica significativa.

4.1.3 [Both] Privacy Lead / PIMS Manager deve documentare in REG01 le parti interessate rilevanti e i relativi requisiti PIMS con cadenza annuale ed entro 30 giorni da qualsiasi modifica significativa.

4.1.4 [Both] Privacy Lead / PIMS Manager deve mantenere in REG01 la sintesi delle interazioni dei processi PIMS prima di ciascun riesame della direzione.

4.2 Determinazione del ruolo PIMS

4.2.1 [Both] Process Owner / Business Owner deve classificare in REG02 il ruolo PIMS dell'organizzazione per ciascuna attività di trattamento delle PII prima dell'avvio dell'attività di trattamento.

4.2.2 [Joint Controller] Vendor / Procurement Owner deve documentare in REG08 l'allocazione delle responsabilità tra contitolari del trattamento prima dell'avvio del trattamento congiunto.

4.2.3 [Processor] Vendor / Procurement Owner deve documentare in REG08 le istruzioni di trattamento del cliente per le attività svolte come responsabile del trattamento prima dell'onboarding del servizio.

4.2.4 [Subprocessor] Vendor / Procurement Owner deve documentare in REG08 le istruzioni del cliente a monte e gli accordi approvati di sub-responsabilità prima dell'avvio del trattamento da parte del sub-responsabile.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Eccezioni

9.1 Richiesta e approvazione delle eccezioni

9.1.1 [All] Process Owner / Business Owner deve documentare in REG12 qualsiasi eccezione richiesta alla presente politica prima che si verifichi la deviazione.

9.1.2 [Both] Privacy Lead / PIMS Manager deve valutare in REG04 il rischio privacy di ciascuna eccezione richiesta prima dell'approvazione.

9.1.3 [Both] Top Management deve approvare in REG12 le eccezioni che superano le soglie accettate di rischio privacy prima dell'attuazione.

9.1.4 [Both] Privacy Lead / PIMS Manager deve riesaminare in REG12 le eccezioni PIMS attive con cadenza trimestrale fino alla chiusura.

9.2 Chiusura delle eccezioni

9.2.1 [All] Process Owner / Business Owner deve documentare in REG12 le evidenze di chiusura dell'eccezione entro la data di scadenza approvata dell'eccezione.

9.2.2 [Both] Internal Audit / Compliance Reviewer deve verificare in REG12 le evidenze di chiusura delle eccezioni scadute durante il successivo audit interno pianificato.

10. Applicazione della politica

10.1 Gestione delle non conformità

10.1.1 [All] Privacy Lead / PIMS Manager deve registrare in REG12 le sospette non conformità alla presente politica entro cinque giorni lavorativi dall'identificazione.

10.1.2 [All] Process Owner / Business Owner deve attuare in REG12 le azioni correttive approvate entro la data di scadenza assegnata dopo l'approvazione della non conformità.

10.1.3 [All] Top Management deve riesaminare in REG12 le non conformità PIMS maggiori irrisolte in occasione di ciascun riesame della direzione.

10.1.4 [All] Internal Audit / Compliance Reviewer deve verificare in REG12 l'efficacia delle azioni correttive entro 30 giorni dalla chiusura segnalata.

10.2 Escalation

10.2.1 [All] Privacy Lead / PIMS Manager deve segnalare a Top Management in REG12 le azioni correttive maggiori scadute entro cinque giorni lavorativi dopo la data di scadenza.

10.2.2 [All] Top Management deve registrare in REG12 le decisioni sulle azioni correttive maggiori scadute entro 15 giorni lavorativi dall'escalation.

11. Riesame e manutenzione

11.1 Riesame della politica

11.1.1 [All] Privacy Lead / PIMS Manager deve riesaminare la presente politica in REG12 con cadenza annuale ed entro 30 giorni da qualsiasi modifica significativa di natura legale, organizzativa, del trattamento, tecnologica o dell'ambito di certificazione.

11.1.2 [All] Data Protection Officer / Privacy Advisor deve fornire consulenza documentata in REG12 prima dell'approvazione della politica quando cambiano obblighi privacy significativi.

11.1.3 [All] Top Management deve approvare in REG12 le modifiche significative alla presente politica prima della pubblicazione.

11.1.4 [All] Privacy Lead / PIMS Manager deve aggiornare REG01 e REG03 entro 15 giorni lavorativi dalle modifiche approvate della politica che alterano l'ambito di applicazione del PIMS o l'applicabilità dei controlli.

11.1.5 [All] Privacy Lead / PIMS Manager deve registrare in REG11 la comunicazione delle modifiche approvate della politica entro 30 giorni dalla pubblicazione.

12. Politiche correlate

12.1 La presente politica è supportata dalle seguenti politiche correlate:

12.2 PII02 - Politica sui ruoli, le responsabilità e l'accountability privacy

12.3 PII03 - Politica sull'inventario dei trattamenti delle PII e sulla base giuridica

12.4 PII07 - Politica sulla valutazione del rischio privacy e sulla DPIA

12.5 PII08 - Politica sulla privacy by design e by default

12.6 PII12 - Politica su responsabili del trattamento, sub-responsabili e condivisione dei dati

12.7 PII14 - Politica sulla sicurezza delle PII e sul controllo degli accessi

12.8 PII15 - Politica sulla gestione degli incidenti PII e delle violazioni

12.9 PII16 - Politica sulla formazione, la consapevolezza e la competenza privacy

12.10 PII17 - Politica sulla gestione delle informazioni documentate e delle evidenze del PIMS

12.11 PII18 - Politica sul monitoraggio, sull'audit e sul miglioramento del PIMS

13. Standard e quadri di riferimento

13.1 La presente politica è mappata ai seguenti standard e normative. La mappatura spiega in che modo la politica supporta i requisiti citati e identifica le clausole interne che li attuano o li supportano.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Mappata alla determinazione del contesto organizzativo, delle questioni del contesto privacy e dell'applicabilità del ruolo di titolare del trattamento o di responsabile del trattamento per le attività PIMS. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Mappata all'identificazione delle parti interessate, degli interessati, dei clienti, delle autorità di controllo, dei responsabili del trattamento, dei sub-responsabili e dei relativi requisiti PIMS pertinenti. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Mappata alla definizione, approvazione, mantenimento e modifica dell'ambito di applicazione documentato del PIMS. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Mappata all'istituzione, attuazione, mantenimento e miglioramento dei processi PIMS e delle loro interazioni. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Mappata all'approvazione da parte di Top Management, alle risorse, al riesame della governance e alla leadership sull'efficacia e sul miglioramento del PIMS. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Mappata al mantenimento della presente politica privacy come informazione documentata approvata e alla comunicazione delle modifiche della politica. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Mappata all'assegnazione e comunicazione di ruoli, responsabilità e autorità PIMS. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Mappata alla pianificazione delle azioni per rischi e opportunità del PIMS utilizzando il contesto, i requisiti delle parti interessate, gli obiettivi e gli input di miglioramento. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Mappata all'obbligo di valutazione del rischio privacy prima di trattamenti nuovi o modificati in modo significativo e al mantenimento delle evidenze del rischio privacy. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Mappata al trattamento del rischio privacy, alla selezione dei controlli, al collegamento con il programma di sicurezza delle informazioni e al mantenimento della Dichiarazione di Applicabilità. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Mappata all'istituzione, misurazione, monitoraggio, comunicazione e aggiornamento degli obiettivi PIMS. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Mappata alle modifiche pianificate del PIMS e al controllo delle modifiche che incidono su ambito di applicazione, ruoli, controlli e informazioni documentate. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Mappata alla determinazione e messa a disposizione delle risorse per l'istituzione, l'operatività, il mantenimento e il miglioramento del PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Mappata alle aspettative di competenza e alle evidenze a supporto delle responsabilità PIMS e dello svolgimento dei ruoli. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Mappata alla consapevolezza della politica privacy, al contributo all'efficacia del PIMS e alle implicazioni della non conformità. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Mappata alle comunicazioni interne ed esterne pertinenti alla governance del PIMS, alle modifiche della politica e all'escalation. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Mappata alla creazione, mantenimento, controllo, disponibilità per l'audit e conservazione delle informazioni documentate. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Mappata alla pianificazione, attuazione e controllo dei processi operativi PIMS e dei processi forniti esternamente. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Mappata all'esecuzione delle valutazioni del rischio privacy a intervalli pianificati e quando modifiche significative sono proposte o si verificano. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Mappata all'attuazione dei piani di trattamento del rischio privacy e alla conservazione delle evidenze dei risultati del trattamento. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Mappata a monitoraggio, misurazione, analisi, valutazione, metriche e reportistica sull'efficacia del PIMS. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Mappata alla pianificazione degli audit interni, al campionamento delle evidenze, ai risultati degli audit e al riesame indipendente. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Mappata agli input del riesame della direzione, al riesame delle prestazioni, agli output del riesame della direzione e alle decisioni di miglioramento. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Mappata al miglioramento continuo mediante riesame della direzione, metriche, monitoraggio delle azioni correttive e mantenimento della politica. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Mappata alla gestione delle non conformità, alle azioni correttive, all'escalation, alla chiusura e alla verifica dell'efficacia. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mappata alle registrazioni lato titolare del trattamento relative alle finalità di trattamento, al collegamento con la base giuridica, alla determinazione della necessità della DPIA, all'allocazione delle responsabilità tra contitolari del trattamento e alle registrazioni delle evidenze del trattamento. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Mappata agli accordi con i clienti del responsabile del trattamento, alle istruzioni documentate del cliente e alle limitazioni delle finalità del responsabile del trattamento. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Mappata al collegamento con la politica di sicurezza delle PII, alla titolarità della baseline dei controlli di sicurezza delle PII e allo stato dei controlli di sicurezza delle informazioni nella Dichiarazione di Applicabilità del PIMS. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mappato alle evidenze di accountability, all'approvazione della politica, alla classificazione dei ruoli di trattamento, all'applicabilità dei controlli, al monitoraggio, all'audit e alle registrazioni delle azioni correttive. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Mappato alle misure di governance del titolare del trattamento, all'approvazione della politica, agli obiettivi PIMS, al riesame dell'efficacia e alle evidenze documentate dell'accountability del titolare del trattamento. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Mappato alla determinazione e documentazione dell'allocazione delle responsabilità tra contitolari del trattamento prima dell'avvio del trattamento congiunto. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Mappato alle registrazioni di governance di responsabili del trattamento e sub-responsabili, alle istruzioni di trattamento del cliente e al controllo dei processi forniti esternamente. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Mappato alle registrazioni delle attività di trattamento, alla classificazione dei ruoli, alle registrazioni di accountability del trattamento e alle evidenze conservate per la verificabilità in sede di audit. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Mappato alla governance della baseline di sicurezza delle PII, alla titolarità dei controlli di sicurezza, allo stato di attuazione della sicurezza e alla conferma dei controlli operativi. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35 -** Mappato alla determinazione della necessità della DPIA e alla valutazione del rischio privacy prima che proceda un trattamento in qualità di titolare del trattamento ad alto rischio o modificato in modo significativo. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Mappata all'identificazione dei controlli privacy, ai principi privacy, alla sicurezza delle informazioni, alla conformità privacy, all'audit, alle evidenze e alla governance privacy basata sul rischio. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mappata alla governance PIA, alla determinazione dei trigger DPIA, alla preparazione della PIA, ai criteri di rischio privacy e alle evidenze documentate della valutazione del rischio privacy. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Mappata ai requisiti del programma di protezione delle PII, all'identificazione dei requisiti di protezione delle PII, alla selezione dei controlli basata sul rischio privacy e all'indirizzo della politica di protezione delle PII. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mappata ai principi di rischio privacy organizzativo, all'impegno della leadership, all'integrazione del rischio privacy nella governance del PIMS e alla comprensione del ruolo dell'organizzazione nel trattamento delle PII. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].