					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII02					Titolo del documento: **Politica sui ruoli, le responsabilità e la responsabilizzazione in materia di 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 / Normativa	Clausola / Controllo / Articolo	Applicabilità	Tipo di copertura	Commento
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Contesto dei ruoli PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Leadership e responsabilizzazione
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Ruoli, responsabilità e autorità PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competenza relativa ai ruoli
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Consapevolezza relativa ai ruoli
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Comunicazione relativa ai ruoli
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informazioni documentate relative ai ruoli
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Titolarità dei controlli operativi
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Ruolo di audit indipendente
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Riesame della direzione sulla responsabilizzazione
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Non conformità e azioni correttive relative ai ruoli
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Responsabilità contrattuale del responsabile del trattamento
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Ruoli e responsabilità dei contitolari del trattamento
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registrazioni di responsabilizzazione
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Accordi e istruzioni del cliente per il responsabile del trattamento
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Allineamento delle finalità del

				responsabile del trattamento
GDPR	Article 5(2)	Controller	Supporting	Evidenze di responsabilizzazione
GDPR	Article 24	Controller	Supporting	Responsabilità e misure del titolare del trattamento
GDPR	Article 26	Joint Controller	Supporting	Accordi tra contitolari del trattamento
GDPR	Article 28	Both	Supporting	Governance dei responsabili del trattamento e istruzioni
GDPR	Article 30	Both	Supporting	Registrazioni dei trattamenti ed evidenze delle responsabilità
GDPR	Article 37	Conditional	Referenced	Designazione del DPO ove applicabile
GDPR	Article 38	Conditional	Supporting	Posizione e indipendenza del DPO ove applicabile
GDPR	Article 39	Conditional	Supporting	Compiti del DPO ove applicabile
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Attori e ruoli del quadro di riferimento per la privacy
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Responsabilizzazione della conformità privacy
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Ruoli per la protezione della PII e separazione dei compiti
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Ruoli e responsabilità per la sicurezza delle informazioni
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Separazione dei compiti

1. Ambito di applicazione

1.1 La presente politica definisce il modello dei ruoli PIMS, la struttura di responsabilizzazione, le regole di assegnazione delle responsabilità, le regole di combinazione dei ruoli, le aspettative di escalation e i requisiti di evidenza per la governance della privacy.

1.2 La presente politica si applica a personale, funzioni, sistemi, fornitori, responsabili del trattamento, sub-responsabili e rapporti di contitolarità del trattamento che partecipano al trattamento di PII o lo influenzano nell'ambito di applicazione del PIMS.

1.3 La presente politica si applica nei contesti di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile.

1.4 La presente politica non crea nuovi titoli organizzativi. Definisce ruoli PIMS canonici che possono essere assegnati a personale o funzioni esistenti, a condizione che l'assegnazione dei ruoli, la competenza, l'indipendenza e i requisiti relativi ai conflitti di interessi siano documentati.

2. Finalità

2.1 La finalità della presente politica è garantire che le responsabilità PIMS siano chiaramente assegnate, comprese, comunicate, comprovate da evidenze, riesaminate e migliorate.

2.2 La presente politica consente all'organizzazione di dimostrare la responsabilizzazione per la governance della privacy, la titolarità operativa del trattamento di PII, la determinazione dei ruoli di titolare e responsabile del trattamento, l'allocazione delle responsabilità tra contitolari del trattamento, la gestione delle istruzioni del responsabile del trattamento, la responsabilità privacy dei fornitori, il riesame indipendente e l'escalation basata sui ruoli.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 definire i ruoli PIMS canonici utilizzati nell'insieme delle politiche PIMS;

3.1.2 garantire che a ogni responsabilità PIMS rilevante sia assegnato un ruolo responsabile;

3.1.3 supportare la responsabilizzazione del titolare del trattamento, del contitolare del trattamento, del responsabile del trattamento e del sub-responsabile;

3.1.4 consentire una combinazione pratica dei ruoli per le piccole e medie organizzazioni, mantenendo sotto controllo i conflitti di interessi;

3.1.5 preservare il riesame indipendente da parte di Internal Audit / Compliance Reviewer;

3.1.6 garantire che le assegnazioni dei ruoli e le modifiche dei ruoli siano registrate negli oggetti di evidenza canonici;

3.1.7 garantire che i titolari dei ruoli PIMS ricevano comunicazioni e attività di sensibilizzazione appropriate;

3.1.8 garantire che lacune, conflitti e non conformità relativi ai ruoli siano oggetto di escalation e corretti.

4. Dichiarazioni della politica

4.1 Modello e assegnazione dei ruoli PIMS

4.1.1 [All] Top Management deve approvare il modello canonico dei ruoli PIMS in REG01 prima dell'attuazione iniziale del PIMS e successivamente con cadenza annuale.

4.1.2 [All] Privacy Lead / PIMS Manager deve mantenere in REG01 le assegnazioni nominative dei ruoli PIMS prima dell'attuazione del PIMS ed entro 10 giorni lavorativi da modifiche del personale o dell'organizzazione.

4.1.3 [All] Privacy Lead / PIMS Manager deve documentare in REG01 l'ambito di responsabilità e il livello di autorità per ciascun ruolo PIMS assegnato prima che l'assegnazione abbia effetto.

4.1.4 [All] Process Owner / Business Owner deve assegnare in REG02 un referente responsabile per ciascuna attività di trattamento di PII prima dell'avvio dell'attività di trattamento.

4.1.5 [All] System Owner / Application Owner deve documentare in REG02 il proprietario del sistema responsabile per ciascun sistema che tratta PII prima della messa in esercizio del sistema.

4.1.6 [All] Vendor / Procurement Owner deve documentare in REG08 il responsabile del rapporto per ciascun responsabile del trattamento, sub-responsabile, condivisione di dati con terze parti o rapporto di contitolarità del trattamento prima dell'onboarding o dell'approvazione dell'accordo.

4.2 Combinazione dei ruoli, separazione e indipendenza

4.2.1 [All] Privacy Lead / PIMS Manager deve documentare in REG01 ciascuna combinazione di ruoli PIMS prima che la combinazione dei ruoli abbia effetto.

4.2.2 [All] Top Management deve approvare in REG01, prima dell'assegnazione, le combinazioni di ruoli che coinvolgono Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator o Internal Audit / Compliance Reviewer.

4.2.3 [All] Internal Audit / Compliance Reviewer deve documentare in REG12 l'indipendenza dal processo PIMS oggetto di riesame prima dell'avvio di ciascun audit PIMS o riesame di conformità.

4.2.4 [All] Privacy Lead / PIMS Manager deve registrare in REG12 i controlli compensativi per i conflitti di separazione inevitabili prima di approvare una combinazione di ruoli.

4.2.5 [All] Data Protection Officer / Privacy Advisor deve registrare in REG12 le criticità relative all'indipendenza del ruolo o ai conflitti di interessi entro cinque giorni lavorativi dall'identificazione.

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

9. Eccezioni

9.1.1 [All] Process Owner / Business Owner deve richiedere in REG12 un'eccezione alla responsabilizzazione dei ruoli prima di operare un'attività di trattamento di PII senza un ruolo assegnato richiesto.

9.1.2 [All] Privacy Lead / PIMS Manager deve valutare in REG12 l'impatto e la mitigazione di ciascuna eccezione alla responsabilizzazione dei ruoli entro 10 giorni lavorativi dalla richiesta.

9.1.3 [All] Top Management deve approvare in REG12 le eccezioni alla responsabilizzazione dei ruoli superiori a 30 giorni o che incidono su trattamenti ad alto rischio prima che l'eccezione abbia effetto.

9.1.4 [All] Privacy Lead / PIMS Manager deve fissare in REG12 una data di scadenza non superiore a 90 giorni per ciascuna eccezione approvata alla responsabilizzazione dei ruoli prima dell'approvazione.

9.1.5 [All] Privacy Lead / PIMS Manager deve chiudere o rivalutare in REG12 ciascuna eccezione alla responsabilizzazione dei ruoli entro cinque giorni lavorativi dalla scadenza.

10. Applicazione

10.1.1 [All] Privacy Lead / PIMS Manager deve registrare in REG12 le assegnazioni dei ruoli PIMS mancanti, inesatte o obsolete come non conformità entro cinque giorni lavorativi dall'identificazione.

10.1.2 [All] Top Management deve richiedere in REG12 un'azione correttiva entro 15 giorni lavorativi per fallimenti della responsabilizzazione ripetuti o prolungati.

10.1.3 [All] Process Owner / Business Owner deve impedire la messa in esercizio di trattamenti di PII nuovi o modificati quando le evidenze richieste relative ai ruoli e alla responsabilizzazione sono assenti da REG02 o REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer deve verificare in REG12 l'efficacia delle azioni correttive per le non conformità relative alla responsabilizzazione dei ruoli al successivo audit pianificato o entro 60 giorni dalla chiusura, a seconda di quale evento si verifichi per primo.

11. Riesame e manutenzione

11.1.1 [All] Privacy Lead / PIMS Manager deve riesaminare la presente politica annualmente ed entro 30 giorni da modifiche rilevanti al modello dei ruoli PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor deve riesaminare in REG12 le modifiche proposte alla presente politica per valutarne l'impatto sui ruoli privacy prima dell'approvazione.

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

11.1.4 [All] Privacy Lead / PIMS Manager deve aggiornare REG01 e REG11 entro 15 giorni lavorativi dalle modifiche approvate ai ruoli, alle responsabilità o ai requisiti di comunicazione PIMS.

12. Politiche correlate

12.1 La presente politica è supportata dalle seguenti politiche correlate:

12.2 PII01 - Politica del Sistema di gestione delle informazioni sulla privacy

12.3 PII03 - Politica sull'inventario dei trattamenti di 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 di gestione privacy di responsabili del trattamento, sub-responsabili e terze parti

12.7 PII14 - Politica di sicurezza della PII e controllo degli accessi

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

12.9 PII16 - Politica di formazione, sensibilizzazione e competenza in materia di privacy

12.10 PII17 - Politica di gestione delle informazioni documentate e delle evidenze PIMS

12.11 PII18 - Politica di monitoraggio, audit e 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 dei ruoli PIMS, dell'applicabilità ai titolari e ai responsabili del trattamento, della titolarità del trattamento e delle registrazioni delle responsabilità relative ai rapporti. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Mappata all'approvazione da parte di Top Management, alla supervisione della responsabilizzazione, al riesame annuale della direzione, alle metriche di responsabilizzazione e alle azioni correttive per i fallimenti relativi ai ruoli. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Mappata all'assegnazione, documentazione, comunicazione e mantenimento dei ruoli, delle responsabilità e delle autorità PIMS, della titolarità dei sistemi, della titolarità del

trattamento, della titolarità dei rapporti con i fornitori, della titolarità dell'escalation degli incidenti e della responsabilità del riesame indipendente. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Mappata alle evidenze di competenza e sensibilizzazione specifiche per il ruolo per le responsabilità PIMS assegnate. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Mappata alla consapevolezza delle responsabilità PIMS assegnate, alle evidenze di presa d'atto e alla reportistica annuale sulla sensibilizzazione relativa ai ruoli. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Mappata alla comunicazione delle assegnazioni dei ruoli, delle modifiche dei ruoli, delle escalation e delle informazioni di passaggio di consegne dei ruoli. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Mappata alle informazioni documentate relative alle assegnazioni dei ruoli PIMS, agli ambiti di responsabilità, ai livelli di autorità, alla conservazione annuale delle evidenze e al mantenimento della matrice dei ruoli. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Mappata alla titolarità dei controlli operativi per attività di trattamento, sistemi, fornitori, responsabili del trattamento, sub-responsabili, rapporti di contitolarità del trattamento e controlli di messa in esercizio. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Mappata all'audit indipendente e al riesame di conformità delle evidenze di assegnazione dei ruoli, delle evidenze di combinazione dei ruoli, delle evidenze di indipendenza, delle risultanze e della chiusura delle azioni correttive. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Mappata al riesame della direzione sulla completezza delle assegnazioni dei ruoli PIMS, sui conflitti di ruolo, sulle eccezioni, sulle metriche di responsabilizzazione e sugli output del riesame della responsabilizzazione. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Mappata a escalation, registrazione delle non conformità, azioni correttive, chiusura delle eccezioni e verifica dell'efficacia per le problematiche di responsabilizzazione dei ruoli. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Mappata all'assegnazione e alla documentazione della responsabilità contrattuale del responsabile del trattamento e dell'escalation delle responsabilità delle terze parti prima dell'approvazione o del rinnovo del contratto. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Mappata alla documentazione dell'allocazione delle responsabilità tra contitolari del trattamento e delle evidenze delle responsabilità relative ai rapporti prima dell'avvio del trattamento in contitolarità. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Mappata al mantenimento delle registrazioni di responsabilizzazione per la titolarità del trattamento da parte del titolare, la classificazione dei ruoli e la titolarità delle evidenze. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Mappata alla responsabilità dell'accordo con il cliente del responsabile del trattamento, alla titolarità delle istruzioni del cliente e alle evidenze dei rapporti del responsabile del trattamento. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Mappata all'allineamento delle finalità e delle istruzioni del responsabile del trattamento mediante la titolarità delle istruzioni del cliente e la verifica dei ruoli di titolare e responsabile del trattamento. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Mappata alle evidenze di responsabilizzazione per assegnazioni dei ruoli, titolarità del trattamento, riesami dei ruoli, non conformità e risultanze di audit. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mappata alla responsabilità del titolare del trattamento, alla titolarità responsabile del trattamento, alla supervisione di Top Management, al riesame annuale e alle misure di responsabilizzazione. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Mappata alla documentazione dell'allocazione delle responsabilità tra contitolari del trattamento e delle evidenze delle responsabilità relative ai rapporti prima dell'avvio del trattamento in contitolarità. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Mappata all'allocazione delle responsabilità di responsabili del trattamento e sub-responsabili, alla titolarità delle istruzioni del cliente, alla responsabilità contrattuale e ai percorsi di escalation delle terze parti. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Mappata alle registrazioni dei trattamenti, alla titolarità del trattamento, alla classificazione dei ruoli PIMS e alla verifica dei ruoli di titolare e responsabile del trattamento. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Mappata alla documentazione del ruolo Data Protection Officer / Privacy Advisor quando la designazione è applicabile o attribuita volontariamente. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Mappata alla posizione, indipendenza, coinvolgimento e gestione dei conflitti di interessi di Data Protection Officer / Privacy Advisor ove applicabile. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Mappata al parere privacy, alle osservazioni di monitoraggio, al riesame consultivo e al riesame dell'impatto privacy relativo ai ruoli da parte di Data Protection Officer / Privacy Advisor ove applicabile. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Mappata agli attori del quadro di riferimento per la privacy e all'allocazione dei ruoli per interessati, titolari del trattamento di PII, responsabili del trattamento di PII, terze parti e classificazione dei ruoli PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Mappata alla responsabilizzazione della conformità privacy, alle evidenze dei ruoli, al riesame, alle risultanze di audit e alla verifica delle azioni correttive. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Mappata alla definizione dei ruoli di protezione della PII, alla documentazione dei ruoli, alla comunicazione dei ruoli, al coordinamento tra sicurezza e privacy e alla separazione dei compiti per la protezione della PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Mappata alla definizione, allocazione, documentazione, comunicazione e mantenimento delle responsabilità PIMS e di sicurezza delle informazioni. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Mappata alla separazione dei compiti, all'approvazione della combinazione dei ruoli, al riesame indipendente, ai controlli sui conflitti e alla verifica delle azioni correttive per i conflitti di ruolo. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].