					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII17					Titolo del documento: **Politica di gestione delle informazioni documentate e delle evidenze del PIMS**							
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 6.1.3	Both	Supporting	Informazioni documentate SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informazioni documentate del PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Controllo delle evidenze operative
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Evidenze di monitoraggio
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Evidenze dell'audit
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Evidenze del riesame della direzione
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Evidenze di non conformità e azione correttiva
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registrazioni del trattamento del titolare del trattamento
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Evidenze degli accordi e delle istruzioni del responsabile del trattamento
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Protezione delle registrazioni
GDPR	Article 5(2)	Controller	Supporting	Evidenze di responsabilizzazione
GDPR	Article 24	Controller	Supporting	Misure ed evidenze del titolare del trattamento
GDPR	Article 28	Both	Supporting	Documentazione del responsabile del trattamento
GDPR	Article 30	Both	Supporting	Registrazioni dei trattamenti
GDPR	Article 32	Both	Supporting	Protezione delle evidenze

ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Evidenze di conformità privacy
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Protezione delle registrazioni
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Controllo delle informazioni documentate
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Protezione delle registrazioni
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Protezione della privacy e dei PII

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti obbligatori per creare, approvare, versionare, proteggere, conservare, reperire, tradurre, ritirare e comprovare le informazioni documentate del PIMS.

1.2 La presente politica si applica alle politiche del PIMS, ai registri, alle approvazioni documentate, alle registrazioni delle evidenze, alle evidenze dell'audit, alle registrazioni del riesame della direzione, alle evidenze delle azioni correttive e alle traduzioni controllate utilizzate per dimostrare la conformità del PIMS.

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

1.4 La presente politica non istituisce un registro separato di controllo documentale. Le evidenze del controllo delle informazioni documentate sono mantenute tramite gli elementi di evidenza canonici del PIMS da REG01 a REG12, con REG03 e REG12 utilizzati per le evidenze relative ad applicabilità dei controlli, audit, non conformità, azioni correttive e miglioramento.

2. Finalità

2.1 La finalità della presente politica è assicurare che le informazioni documentate del PIMS siano accurate, controllate, accessibili agli utenti autorizzati, protette da modifiche o comunicazioni non autorizzate, conservate per garantire la verificabilità e ritirate quando obsolete.

2.2 La presente politica supporta la preparazione alle certificazioni assicurando che le evidenze necessarie a dimostrare la conformità del PIMS possano essere localizzate, verificate, reperite e collegate alle politiche, ai controlli, alle attività di trattamento, ai rischi, agli audit e alle azioni correttive applicabili.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 definire i requisiti di controllo delle informazioni documentate del PIMS;

3.1.2 mantenere l'integrità delle evidenze da REG01 a REG12;

3.1.3 assicurare la tracciabilità dell'approvazione delle politiche e delle evidenze;

3.1.4 assicurare che la cronologia delle versioni e le decisioni di ritiro siano documentate;

3.1.5 collegare le evidenze del PIMS alla Dichiarazione di Applicabilità e alle mappature delle politiche;

3.1.6 controllare l'accesso ai documenti e alle registrazioni delle evidenze del PIMS;

3.1.7 supportare il controllo delle versioni di politiche ed evidenze multilingue;

3.1.8 consentire il tempestivo reperimento delle evidenze dell'audit;

3.1.9 evitare burocrazia non necessaria nel controllo documentale;

3.1.10 preservare registrazioni pronte per l'audit ai fini di certificazione, assurance dei clienti e miglioramento continuo.

4. Dichiarazioni della politica

4.1 Controllo delle informazioni documentate del PIMS

4.1.1 [All] Il Privacy Lead / PIMS Manager deve mantenere un indice delle informazioni documentate del PIMS in REG12 prima della pubblicazione iniziale del PIMS e successivamente con cadenza trimestrale.

4.1.2 [All] Il Process Owner / Business Owner deve identificare in REG02 le informazioni documentate richieste per ciascuna attività di trattamento di PII di sua competenza prima dell'avvio dell'attività di trattamento e successivamente con cadenza annuale.

4.1.3 [All] Il Privacy Lead / PIMS Manager deve collegare le politiche, i controlli e gli obblighi di evidenza applicabili del PIMS a REG03 prima di ogni rilascio di politica ed entro 15 giorni lavorativi da qualsiasi modifica sostanziale dell'applicabilità dei controlli.

4.1.4 [All] Il Privacy Lead / PIMS Manager deve assegnare in REG12 un livello di accesso e una classificazione della sensibilità delle evidenze a ciascuna categoria di informazioni documentate del PIMS prima che la categoria sia utilizzata.

4.2 Creazione, approvazione, versionamento e pubblicazione

4.2.1 [All] Il Privacy Lead / PIMS Manager deve assegnare in REG12 un identificativo del documento, un proprietario, un numero di versione, lo stato di approvazione, la data di efficacia e la data di riesame prima di pubblicare informazioni documentate del PIMS.

4.2.2 [All] Top Management deve approvare in REG12 le politiche core del PIMS e le modifiche sostanziali alle politiche prima della pubblicazione.

4.2.3 [All] Il Privacy Lead / PIMS Manager deve approvare in REG12 i modelli di evidenza del PIMS o le sezioni integrate dei registri prima dell'uso operativo.

4.2.4 [All] Il Privacy Lead / PIMS Manager deve registrare in REG12 la cronologia delle versioni e la motivazione delle modifiche prima di rilasciare informazioni documentate del PIMS aggiornate.

4.2.5 [All] Il Privacy Lead / PIMS Manager deve registrare in REG11 la comunicazione delle modifiche approvate alle informazioni documentate del PIMS entro 30 giorni dalla pubblicazione.

[... 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] Il Process Owner / Business Owner deve richiedere in REG12 le eccezioni relative alle informazioni documentate o al controllo delle evidenze prima di discostarsi dalla presente politica.

9.1.2 [All] Il Privacy Lead / PIMS Manager deve valutare in REG12 ciascuna eccezione relativa alle informazioni documentate o al controllo delle evidenze entro 10 giorni lavorativi dalla richiesta.

9.1.3 [All] Il Data Protection Officer / Privacy Advisor deve registrare il parere in REG12 prima dell'approvazione di qualsiasi eccezione che riguardi la comunicazione di evidenze contenenti PII, una discrepanza di traduzione, un conflitto di conservazione o una limitazione delle evidenze dell'audit.

9.1.4 [All] Top Management deve approvare in REG12 le eccezioni relative alle informazioni documentate superiori a 30 giorni o che incidano sulla certificazione, sui trattamenti ad alto rischio o sull'assurance esterna prima che l'eccezione produca effetti.

9.1.5 [All] Il Privacy Lead / PIMS Manager deve impostare in REG12 una data di scadenza non superiore a 90 giorni per ciascuna eccezione approvata relativa alle informazioni documentate o al controllo delle evidenze.

9.1.6 [All] Il Privacy Lead / PIMS Manager deve chiudere o rivalutare in REG12 ciascuna eccezione relativa alle informazioni documentate o al controllo delle evidenze entro cinque giorni lavorativi dalla scadenza.

10. Applicazione della politica

10.1.1 [All] Il Privacy Lead / PIMS Manager deve registrare in REG12 le informazioni documentate del PIMS mancanti, inaccurate, non controllate, obsolete o non reperibili come non conformità entro cinque giorni lavorativi dall'identificazione.

10.1.2 [All] Il Privacy Lead / PIMS Manager deve impedire la pubblicazione di informazioni documentate del PIMS quando le evidenze richieste di approvazione, versione, proprietario o data di efficacia mancano da REG12.

10.1.3 [All] Il Process Owner / Business Owner deve impedire la presentazione ai fini di audit delle evidenze di trattamento quando le evidenze richieste relative a proprietario, data, stato o approvazione mancano da REG02.

10.1.4 [All] Il System Owner / Application Owner deve rimuovere gli accessi non autorizzati ai repository delle informazioni documentate del PIMS e registrare la rimozione in REG12 entro un giorno lavorativo dall'identificazione.

10.1.5 [All] L'Internal Audit / Compliance Reviewer deve verificare in REG12 l'efficacia delle azioni correttive per le non conformità relative alle informazioni documentate al successivo audit programmato o entro 60 giorni dalla chiusura, se precedente.

11. Riesame e manutenzione

11.1.1 [All] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica con cadenza annuale ed entro 30 giorni da una modifica sostanziale dei requisiti relativi alle informazioni documentate del PIMS.

11.1.2 [All] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica entro 30 giorni da una risultanza di audit rilevante, una non conformità di certificazione, una modifica della piattaforma di repository o una modifica del processo di pubblicazione multilingue.

11.1.3 [All] Il Data Protection Officer / Privacy Advisor deve riesaminare in REG12 le modifiche significative per la privacy alla presente politica prima dell'approvazione.

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

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

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 PII02 - Politica sui ruoli, le responsabilità e la responsabilizzazione in materia di privacy

12.4 PII03 - Politica sull'inventario dei trattamenti di PII e sulla base giuridica

12.5 PII04 - Politica sull'informativa privacy e sulla trasparenza

12.6 PII05 - Politica di gestione del consenso e delle preferenze

12.7 PII06 - Politica di gestione dei diritti dell'interessato

12.8 PII07 - Politica di valutazione del rischio privacy e DPIA

12.9 PII08 - Politica di privacy by design e privacy by default

12.10 PII09 - Politica di raccolta, uso, comunicazione e condivisione dei PII

12.11 PII10 - Politica di conservazione, cancellazione e smaltimento dei PII

12.12 PII11 - Politica di accuratezza e qualità dei PII

12.13 PII12 - Politica di gestione privacy di responsabili del trattamento, sub-responsabili e terze parti

12.14 PII13 - Politica sui trasferimenti internazionali di PII

12.15 PII14 - Politica di sicurezza e controllo degli accessi ai PII

12.16 PII15 - Politica di gestione degli incidenti e delle violazioni relativi ai PII

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

12.18 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 regolamenti. 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 6.1.3** - Mappata al mantenimento della Dichiarazione di Applicabilità del PIMS, delle registrazioni di applicabilità dei controlli e del collegamento tra politiche ed evidenze. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Mappata all'identificazione delle informazioni documentate, all'approvazione, al controllo delle versioni, all'accesso, al reperimento, alla preservazione, al ritiro, al collegamento delle versioni tradotte e ai metadati di conservazione. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Mappata alla pianificazione e al controllo operativi delle evidenze per le registrazioni dei trattamenti, i modelli di evidenza, la qualità delle evidenze operative e le evidenze fornite esternamente. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Mappata al mantenimento di evidenze documentate di misurazione, prestazioni di reperimento, lacune nelle evidenze, mancate corrispondenze nelle traduzioni e completamento del riesame degli accessi ai repository. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Mappata al reperimento delle evidenze dell'audit, al campionamento dell'audit, alla tracciabilità delle evidenze dell'audit e alle risultanze dell'audit relative al controllo delle informazioni documentate. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Mappata alle evidenze del riesame della direzione, alla considerazione del controllo delle informazioni documentate nel riesame della direzione e al riesame, da parte di Top Management, delle prestazioni del controllo delle evidenze. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Mappata alle non conformità relative alle informazioni documentate, alle azioni correttive, alla gestione delle eccezioni, alla chiusura e alla verifica di efficacia. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Mappata alle registrazioni dei trattamenti del titolare del trattamento, alle registrazioni di responsabilizzazione, alla qualità delle evidenze di trattamento e alla conservazione delle evidenze a supporto degli obblighi del titolare del trattamento. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Mappata agli accordi del responsabile del trattamento, alle istruzioni del cliente, alle evidenze fornite esternamente e al controllo delle evidenze del rapporto con il responsabile del trattamento. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Mappata alla protezione delle registrazioni del PIMS contro perdita, modifica non autorizzata, accesso non autorizzato, rilascio non autorizzato e smaltimento improprio. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mappata alle evidenze di responsabilizzazione, alla tracciabilità delle evidenze, al reperimento delle evidenze, alle registrazioni di non conformità e alle registrazioni pronte per l'audit che dimostrano la conformità. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Mappata alle evidenze di governance del titolare del trattamento, alle registrazioni di approvazione, al controllo delle politiche, alle misure di responsabilizzazione, al riesame documentato e alla supervisione di Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Mappata alla documentazione di responsabili del trattamento e sub-responsabili, alle evidenze delle istruzioni del cliente, alle evidenze di processo fornite esternamente e al controllo della comunicazione delle evidenze. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Mappata alle evidenze delle registrazioni dei trattamenti, ai requisiti di qualità delle evidenze, ai riferimenti alle attività di trattamento e ai metadati di proprietario/stato delle evidenze di trattamento. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Mappata alla protezione dei repository delle evidenze, alle restrizioni di accesso, alle approvazioni degli accessi, al riesame della protezione dei repository e alla rimozione degli accessi non autorizzati. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mappata alle evidenze di conformità privacy, al reperimento delle evidenze dell'audit, alla tracciabilità delle evidenze, al supporto al riesame indipendente e alle evidenze delle azioni correttive. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Mappata alla protezione delle registrazioni relative ai PII, alla preservazione delle registrazioni e ai controlli di accesso e cancellazione dei repository delle evidenze. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Mappata all'identificazione delle informazioni documentate, all'approvazione, alla disponibilità, alla protezione, al controllo delle versioni, alla conservazione, alla destinazione finale e al controllo delle informazioni documentate richieste esternamente. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Mappata alla protezione delle registrazioni del PIMS contro perdita, distruzione, falsificazione, accesso non autorizzato, rilascio non autorizzato e smaltimento improprio. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Mappata alla protezione della privacy e dei PII nelle informazioni documentate, nei repository delle evidenze, nelle comunicazioni e nelle registrazioni ad accesso controllato. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].