					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII09					Titolo del documento: **Politica di raccolta, uso, comunicazione e condivisione delle PII**							
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 7.5; Clause 8.1	Both	Primary	Controllo operativo documentato
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoraggio e azione correttiva
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Finalità e registrazioni dei trattamenti
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Collegamento alla base giuridica
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Responsabilità di condivisione tra contitolari del trattamento
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Limiti di raccolta, trattamento e minimizzazione
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Collegamento dell'instradamento dei trasferimenti
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registrazioni dei trasferimenti e delle comunicazioni
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Istruzioni e registrazioni del responsabile del trattamento
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Collegamento dell'instradamento dei trasferimenti del responsabile del trattamento
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Registrazioni e richieste di comunicazione del responsabile del trattamento
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Limitazione delle finalità, minimizzazione e responsabilizzazione

GDPR	Article 6	Controller	Referenced	Collegamento alla base giuridica
GDPR	Article 24	Controller	Supporting	Responsabilità del titolare del trattamento
GDPR	Article 26	Joint Controller	Supporting	Accordi tra contitolari del trattamento
GDPR	Article 28	Both	Supporting	Istruzioni del responsabile del trattamento e limiti di comunicazione
GDPR	Article 30	Both	Supporting	Registrazioni dei trattamenti e dei destinatari
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Finalità, raccolta, minimizzazione e limitazione della comunicazione
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Responsabilizzazione e conformità privacy
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Controlli su finalità, raccolta, minimizzazione, uso e comunicazione

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti per raccogliere, utilizzare, comunicare e condividere PII nell'ambito di applicazione del PIMS.

1.2 La presente politica si applica a:

1.2.1 raccolta di PII tramite canali diretti, indiretti, automatizzati, manuali, interni, esterni e di terze parti;

1.2.2 uso interno approvato delle PII da parte di processi aziendali, sistemi e applicazioni;

1.2.3 uso secondario delle PII per una finalità nuova o sostanzialmente modificata;

1.2.4 comunicazione esterna di PII a destinatari, partner, autorità, responsabili del trattamento, sub-responsabili, fornitori e altre terze parti;

1.2.5 accordi ricorrenti di condivisione dei dati e comunicazioni una tantum;

1.2.6 contesti di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile;

1.2.7 REG02 - Inventario dei trattamenti PII / ROPA, REG08 - Registro di responsabili del trattamento, sub-responsabili e condivisione dei dati, REG09 - Registro dei trasferimenti internazionali, e REG12 - Registro di audit, non conformità, azioni correttive e miglioramento.

1.3 La presente politica non sostituisce:

1.3.1 PII03 per la titolarità dell'inventario dei trattamenti, della base giuridica e del ROPA;

1.3.2 PII04 per contenuto, pubblicazione e controllo delle versioni dell'informativa privacy;

1.3.3 PII05 per il funzionamento di consenso e preferenze;

1.3.4 PII06 per la gestione delle richieste di esercizio dei diritti degli interessati;

1.3.5 PII07 per la metodologia DPIA e la valutazione del rischio privacy;

1.3.6 PII08 per i gate di privacy by design;

1.3.7 PII10 per l'esecuzione di conservazione, cancellazione e smaltimento;

1.3.8 PII11 per la gestione dell'accuratezza e della qualità;

1.3.9 PII12 per la governance del ciclo di vita di responsabili del trattamento, sub-responsabili e terze parti;

1.3.10 PII13 per la selezione del meccanismo di trasferimento internazionale e i controlli sul rischio di trasferimento;

1.3.11 PII14 per la sicurezza delle PII e il controllo degli accessi;

1.3.12 PII15 per la gestione di incidenti e violazioni dei dati personali;

1.3.13 PII18 per la governance a livello di PIMS di monitoraggio, audit, non conformità, azione correttiva e miglioramento.

1.4 Ai fini della presente politica:

1.4.1 "uso approvato" indica un uso di PII registrato in REG02 per una specifica attività di trattamento, finalità, categoria di PII, categoria di interessati, titolare dell'attività e ruolo PIMS applicabile.

1.4.2 "raccolta" indica l'acquisizione di PII direttamente da un interessato, indirettamente da un'altra parte, automaticamente da un sistema o dispositivo, oppure tramite una fonte di dati interna o esterna.

1.4.3 "uso secondario" indica l'uso di PII per una finalità non ancora registrata come finalità approvata in REG02 per la relativa attività di trattamento.

1.4.4 "verifica di compatibilità" indica una valutazione documentata in REG02 della finalità originaria, della finalità proposta, della dipendenza dalla base giuridica, delle categorie di PII,

delle aspettative degli interessati, della giustificazione della minimizzazione, dell'impatto della comunicazione o del trasferimento e dell'instradamento verso altre politiche PIMS ove necessario.

1.4.5 "comunicazione esterna" indica il rendere disponibili PII a una parte esterna all'organizzazione o esterna alla catena documentata di istruzioni del cliente.

1.4.6 "condivisione dei dati" indica un accordo ricorrente o strutturato in base al quale PII sono comunicate, trasferite, accedute, scambiate o rese disponibili a un'altra parte.

1.4.7 "condivisione ricorrente sensibile" indica una condivisione ricorrente che coinvolge categorie particolari di PII, PII relative a reati, PII di minori, registrazioni ad alto impatto, condivisione su larga scala o condivisione esterna che coinvolge un luogo di trasferimento registrato in REG09.

2. Finalità

2.1 La finalità della presente politica è assicurare che PII siano raccolte, utilizzate, comunicate e condivise solo per finalità documentate, approvate, limitate e soggette a responsabilizzazione.

2.2 La presente politica consente all'organizzazione di dimostrare che raccolta e uso sono collegati alle registrazioni dei trattamenti in REG02, che le comunicazioni e gli accordi di condivisione dei dati sono registrati in REG08, che l'instradamento dei trasferimenti internazionali è collegato a REG09 e che eccezioni e non conformità sono gestite tramite REG12.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 limitare la raccolta alle PII necessarie per finalità documentate;

3.1.2 assicurare che l'uso interno delle PII sia approvato prima dell'inizio del trattamento;

3.1.3 richiedere verifiche di compatibilità prima dell'uso secondario;

3.1.4 richiedere approvazione ed evidenze prima della comunicazione esterna;

3.1.5 mantenere le evidenze di condivisione dei dati in REG08 senza creare un registro separato di condivisione dei dati;

3.1.6 indirizzare le dipendenze dai trasferimenti internazionali verso REG09 e PII13 senza duplicare i controlli sui meccanismi di trasferimento;

3.1.7 definire la periodicità di riesame della condivisione ricorrente;

3.1.8 mantenere evidenze utilizzabili in sede di audit per raccolta, uso, comunicazione, condivisione, eccezioni e azioni correttive.

4. Dichiarazioni della politica

4.1 Limitazione della raccolta

4.1.1 [Controller] Process Owner / Business Owner DEVE registrare in REG02 la finalità della raccolta, la fonte o il canale, le categorie di PII, le categorie di interessati e gli elementi minimi dei dati prima dell'avvio di qualsiasi nuova attività di raccolta o modifica sostanziale della raccolta.

4.1.2 [Controller] Privacy Lead / PIMS Manager DEVE riesaminare la registrazione della raccolta in REG02 prima dell'inizio della raccolta quando viene aggiunta una nuova categoria di PII, fonte, canale o finalità.

4.1.3 [Controller] Process Owner / Business Owner DEVE registrare in REG02 una giustificazione di necessità per ciascun elemento di dati PII prima che tale elemento sia raccolto.

4.1.4 [Processor] Process Owner / Business Owner DEVE registrare in REG02 il riferimento all'istruzione del cliente da REG08 prima di raccogliere PII per conto di un cliente.

4.1.5 [Joint Controller] Process Owner / Business Owner DEVE registrare in REG08 l'allocazione delle responsabilità di raccolta tra contitolari del trattamento prima dell'avvio della raccolta congiunta.

4.2 Controlli sull'uso interno approvato

4.2.1 [Controller] Process Owner / Business Owner DEVE registrare in REG02 le regole di uso interno approvato per ciascuna attività di trattamento prima dell'inizio dell'uso.

4.2.2 [Controller] System Owner / Application Owner DEVE implementare solo campi di workflow, report o esportazioni per uso interno che abbiano una regola di uso approvato corrispondente in REG02 prima del rilascio in produzione.

4.2.3 [Processor] Process Owner / Business Owner DEVE registrare in REG08 l'allineamento alle istruzioni del cliente prima di utilizzare PII del cliente per qualsiasi attività di responsabile del trattamento o sub-responsabile.

4.2.4 [Controller] Privacy Lead / PIMS Manager DEVE riesaminare le regole di uso approvato in REG02 almeno annualmente per ciascuna attività di trattamento attiva.

4.2.5 [All] Privacy Lead / PIMS Manager DEVE registrare una non conformità in REG12 entro cinque giorni lavorativi quando viene identificato un uso interno non documentato di PII.

[... 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 registrare una richiesta di eccezione in REG12 prima di discostarsi da una regola approvata di raccolta, uso, comunicazione o condivisione.

9.1.2 [All] Privacy Lead / PIMS Manager DEVE registrare una decisione di approvazione o rigetto in REG12 prima che un'eccezione sia attivata.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor DEVE registrare un parere in REG12 prima dell'approvazione di un'eccezione che coinvolga uso secondario incompatibile, condivisione ricorrente sensibile, conflitto relativo a una comunicazione giuridicamente vincolante o instradamento dei trasferimenti.

9.1.4 [All] Top Management DEVE registrare l'approvazione in REG12 prima dell'attivazione di qualsiasi eccezione con durata superiore a 30 giorni di calendario o che interessi più di un'attività di trattamento.

9.1.5 [All] Process Owner / Business Owner DEVE chiudere un'eccezione in REG12 entro la data di scadenza o entro cinque giorni lavorativi dalla cessazione della condizione di eccezione.

10. Applicazione della politica

10.1.1 [All] Privacy Lead / PIMS Manager DEVE registrare raccolta, uso, comunicazione o condivisione non approvati come non conformità in REG12 entro cinque giorni lavorativi dall'identificazione.

10.1.2 [Controller] Process Owner / Business Owner DEVE sospendere raccolta, uso, comunicazione o condivisione entro un giorno lavorativo quando Privacy Lead / PIMS Manager registra in REG12 l'assenza di evidenze REG02 o REG08 approvate.

10.1.3 [Processor] Process Owner / Business Owner DEVE registrare una decisione di arresto o escalation in REG08 e REG12 entro un giorno lavorativo quando PII del cliente sono utilizzate o comunicate al di fuori delle istruzioni documentate.

10.1.4 [All] Top Management DEVE riesaminare in REG12 le non conformità irrisolte ad alto impatto relative a raccolta, uso, comunicazione o condivisione entro 30 giorni di calendario dall'escalation.

10.1.5 [All] Internal Audit / Compliance Reviewer DEVE verificare le evidenze di chiusura delle azioni correttive in REG12 entro 15 giorni lavorativi da quando Privacy Lead / PIMS Manager contrassegna la chiusura.

11. Riesame e manutenzione

11.1.1 [All] Privacy Lead / PIMS Manager DEVE riesaminare la presente politica almeno annualmente e registrare la decisione in REG12.

11.1.2 [All] Privacy Lead / PIMS Manager DEVE riesaminare la presente politica entro 30 giorni di calendario da una modifica sostanziale dell'ambito di applicazione del PIMS, delle finalità del trattamento, del modello di condivisione, dell'instradamento dei trasferimenti o dell'obbligo applicabile e registrare l'esito in REG12.

11.1.3 [All] Process Owner / Business Owner DEVE ricertificare le registrazioni attive REG02 e REG08 almeno annualmente ed entro 30 giorni di calendario da una modifica sostanziale del trattamento.

11.1.4 [All] Internal Audit / Compliance Reviewer DEVE includere i controlli PII09 nel campionamento annuale di audit e registrare la copertura in REG12.

11.1.5 [All] Privacy Lead / PIMS Manager DEVE aggiornare in REG12 i riferimenti alle politiche correlate entro dieci giorni lavorativi quando PII03, PII08, PII10, PII12, PII13, PII14 o PII18 modificano il perimetro operativo della presente politica.

12. Politiche correlate

12.1 La presente politica deve essere letta congiuntamente a:

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

12.3 PII02 - Politica su ruoli, responsabilità e responsabilizzazione privacy

12.4 PII03 - Politica sull'inventario dei trattamenti 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 degli interessati

12.8 PII07 - Politica di valutazione del rischio privacy e DPIA

12.9 PII08 - Politica di privacy by design e by default

12.10 PII10 - Politica di conservazione, cancellazione e smaltimento delle PII

12.11 PII11 - Politica di accuratezza e qualità delle PII

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

12.13 PII13 - Politica sui trasferimenti internazionali di PII

12.14 PII14 - Politica di sicurezza delle PII e controllo degli accessi

12.15 PII15 - Politica di gestione degli incidenti e delle violazioni dei dati personali relativi alle PII

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

12.17 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 supportano.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mappato alle registrazioni operative documentate e al controllo delle evidenze relative a raccolta, uso approvato, uso secondario, comunicazione, condivisione e instradamento dei trasferimenti. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Mappato a monitoraggio, misurazione, riesame, gestione delle eccezioni, non conformità e azione correttiva per i controlli su raccolta, uso, comunicazione e condivisione. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Mappato alle finalità documentate del titolare del trattamento, alle registrazioni degli usi approvati e alle evidenze del trattamento in REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Mappato al collegamento alla base giuridica per raccolta, uso e instradamento dell'uso secondario senza sostituire PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Mappato alle evidenze in REG08 delle responsabilità di raccolta e condivisione tra contitolari del trattamento. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Mappato alla limitazione della raccolta, alla limitazione del trattamento e alla giustificazione della minimizzazione prima che PII siano raccolte o utilizzate. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Mappato al collegamento dell'instradamento dei trasferimenti tramite REG09 senza sostituire i controlli PII13 sui meccanismi di trasferimento. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Mappato alle registrazioni di trasferimenti, comunicazioni e accordi ricorrenti di condivisione dei dati in REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mappato all'allineamento del responsabile del trattamento alle istruzioni del cliente e alle registrazioni del responsabile del trattamento per i limiti di raccolta, uso e uso secondario. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Mappato al collegamento dell'instradamento dei trasferimenti del responsabile del trattamento tramite REG09 senza sostituire i controlli PII13 sui meccanismi di trasferimento. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mappato alle registrazioni delle comunicazioni del responsabile del trattamento, allo stato delle notifiche delle richieste di comunicazione e alle evidenze di autorizzazione alla comunicazione in REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mappato alle evidenze di limitazione delle finalità, minimizzazione dei dati e responsabilizzazione per raccolta, uso, uso secondario, comunicazione e condivisione. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Mappato al collegamento alla base giuridica e all'instradamento per uso secondario nuovo o incompatibile senza sostituire PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Mappato alla governance, alle approvazioni, al riesame e alle misure di responsabilizzazione del titolare del trattamento per raccolta, uso, comunicazione e condivisione. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Mappato alle evidenze delle responsabilità di raccolta e condivisione tra contitolari del trattamento. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Mappato all'allineamento alle istruzioni di responsabili del trattamento e sub-responsabili, all'autorizzazione del cliente e ai limiti di comunicazione. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Mappato alle registrazioni dei trattamenti, dei destinatari, delle comunicazioni e delle condivisioni in REG02 e REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mappato alla specificazione delle finalità, alla limitazione della raccolta, alla minimizzazione dei dati, alla limitazione dell'uso e alla limitazione della comunicazione. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Mappato a responsabilizzazione, evidenze di conformità, riesame, gestione delle eccezioni, campionamento di audit e azione correttiva. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mappato a finalità, limitazione della raccolta, minimizzazione, limitazione dell'uso, limitazione della comunicazione e supporto alle registrazioni delle comunicazioni. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].