					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII16					Titolo del documento: **Politica di formazione, sensibilizzazione e competenza 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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Competenza e consapevolezza
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Comunicazione ed evidenze documentate
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Controllo operativo, misurazione e miglioramento
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Consapevolezza, educazione e formazione sul trattamento dei PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Responsabilizzazione, governance dei responsabili del trattamento, sicurezza e compiti del DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Competenza, consapevolezza e formazione
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Linee guida su consapevolezza, educazione e formazione
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Sicurezza delle informazioni e conformità privacy

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti dell'organizzazione per la formazione, la sensibilizzazione e la competenza in materia di privacy nell'ambito del Sistema di gestione delle informazioni sulla privacy.

1.2 La presente politica si applica al personale, ai contraenti, al personale temporaneo, alle terze parti pertinenti, ai responsabili del trattamento, ai sub-responsabili e alle altre parti interessate il cui lavoro può incidere sul trattamento dei PII, sulle prestazioni del PIMS, sui diritti degli interessati, sul rischio privacy, sulla sicurezza delle informazioni relativa ai PII, sulle istruzioni del responsabile del trattamento, sugli incidenti privacy, sulle informazioni documentate o sulle evidenze di conformità.

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 copre:

1.4.1 identificazione dei destinatari della formazione privacy;

1.4.2 formazione in fase di onboarding;

1.4.3 formazione annuale di aggiornamento;

1.4.4 formazione basata sui ruoli e formazione attivata da eventi;

1.4.5 evidenze di completamento della formazione;

1.4.6 escalation del mancato completamento;

1.4.7 riesame dell'efficacia della formazione;

1.4.8 evidenze di assurance della formazione di responsabili del trattamento, sub-responsabili e terze parti.

1.5 La presente politica non crea una matrice della formazione, un cruscotto della formazione, un registro delle risorse umane, un registro delle competenze, un registro disciplinare o un registro della formazione dei clienti separati. Le assegnazioni della formazione, i completamenti, i promemoria, le evidenze di competenza e le evidenze di sensibilizzazione sono registrati in REG11, mentre eccezioni, escalation, non conformità, azioni correttive ed evidenze di riesame sono registrate in REG12. Le evidenze di assurance della formazione di responsabili del trattamento, sub-responsabili e terze parti sono registrate in REG08 ove pertinente.

1.6 La presente politica non duplica:

1.6.1 l'assegnazione delle responsabilità di ruolo in PII02;

1.6.2 l'inventario dei trattamenti e i requisiti relativi alla base giuridica in PII03;

1.6.3 la metodologia di rischio privacy e DPIA in PII07;

1.6.4 i gate di privacy by design in PII08;

1.6.5 la governance del ciclo di vita dei responsabili del trattamento in PII12;

1.6.6 l'operatività della sicurezza dei PII e del controllo degli accessi in PII14;

1.6.7 il workflow relativo agli incidenti e alle violazioni dei PII in PII15;

1.6.8 la governance delle informazioni documentate in PII17;

1.6.9 la governance del monitoraggio, dell'audit interno e del miglioramento in PII18.

2. Finalità

2.1 La finalità della presente politica è assicurare che le persone il cui lavoro incide sul trattamento dei PII comprendano le proprie responsabilità in materia di privacy, completino una formazione adeguata secondo una cadenza definita, mantengano competenze pertinenti al ruolo e producano evidenze verificabili in sede di audit relative a formazione, sensibilizzazione ed escalation.

2.2 La presente politica sostiene un'attuazione coerente del PIMS utilizzando REG11 come oggetto primario di evidenza per formazione e sensibilizzazione, e REG08, REG10 e REG12 come oggetti di evidenza di supporto.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 definire i destinatari della formazione privacy;

3.1.2 definire i requisiti di formazione in fase di onboarding;

3.1.3 definire i requisiti di formazione annuale di aggiornamento;

3.1.4 definire i requisiti di formazione privacy basata sui ruoli;

3.1.5 registrare le evidenze di completamento in REG11;

3.1.6 gestire l'escalation del mancato completamento tramite REG12;

3.1.7 mantenere in REG08, ove pertinente, le evidenze di assurance della formazione di responsabili del trattamento, sub-responsabili e terze parti;

3.1.8 riesaminare l'efficacia della formazione senza creare metriche eccessive o registri duplicati;

3.1.9 assicurare che i contenuti formativi restino allineati alle politiche PIMS vigenti e agli obblighi privacy sostanziali.

4. Dichiarazioni della politica

4.1 Destinatari e assegnazione della formazione

4.1.1 [All] Il Privacy Lead / PIMS Manager deve definire in REG11 le categorie di destinatari della formazione PIMS prima dell'inizio di ciascun ciclo annuale di formazione.

4.1.2 [All] Il Process Owner / Business Owner deve identificare in REG11 il personale le cui mansioni comportano il trattamento dei PII prima dell'onboarding, dell'assegnazione del ruolo o di una modifica sostanziale delle mansioni.

4.1.3 [Conditional] Il System Owner / Application Owner deve identificare in REG11 gli utenti che richiedono formazione privacy relativa ai sistemi PII, agli accessi privilegiati o all'amministrazione prima che l'accesso sia abilitato o modificato in modo sostanziale.

4.1.4 [Joint Controller] Il Privacy Lead / PIMS Manager deve registrare in REG11 o REG08 l'allocazione delle responsabilità di formazione tra contitolari del trattamento prima che l'attività di trattamento congiunto inizi o subisca modifiche sostanziali.

4.1.5 [Conditional] Il Data Protection Officer / Privacy Advisor deve identificare in REG11 le esigenze di formazione privacy rafforzata prima che la formazione sia assegnata a ruoli che gestiscono trattamenti ad alto rischio, PII di categorie particolari, diritti degli interessati, DPIA, trasferimenti internazionali o valutazioni delle violazioni.

4.1.6 [All] Il Privacy Lead / PIMS Manager deve registrare in REG11 i destinatari assegnati alla formazione, il tipo di formazione, la data di completamento richiesta e il proprietario delle evidenze prima dell'inizio di ciascun ciclo annuale di formazione.

4.2 Cadenza della formazione in fase di onboarding e della formazione annuale

4.2.1 [All] Il Privacy Lead / PIMS Manager deve assegnare in REG11 la formazione di base di sensibilizzazione privacy entro 10 giorni lavorativi dall'onboarding del personale con accesso ai PII o con responsabilità PIMS.

4.2.2 [All] Il Process Owner / Business Owner deve assicurare che il personale assegnato completi in REG11 la formazione privacy in fase di onboarding prima dell'approvazione dell'accesso non supervisionato ai PII o entro 30 giorni dall'onboarding, a seconda di quale evento si verifichi per primo.

4.2.3 [All] Il Privacy Lead / PIMS Manager deve assegnare in REG11 la formazione annuale di aggiornamento privacy almeno una volta ogni 12 mesi.

4.2.4 [All] Il Process Owner / Business Owner deve confermare in REG11 lo stato di completamento della formazione annuale di aggiornamento per il personale assegnato entro la data di scadenza annuale pubblicata.

4.2.5 [Conditional] Il Privacy Lead / PIMS Manager deve assegnare in REG11 una formazione di aggiornamento mirata entro 30 giorni da una modifica sostanziale di una politica privacy, una modifica sostanziale di un processo PIMS, una risultanza dell'audit, un fallimento formativo ricorrente o una lezione pertinente derivante da un incidente relativo ai 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] Il Process Owner / Business Owner deve registrare in REG12 una richiesta di eccezione alla formazione privacy prima che una scadenza di completamento richiesta sia prorogata.

9.1.2 [All] Il Privacy Lead / PIMS Manager deve approvare o respingere in REG12 le richieste di eccezione alla formazione privacy prima che l'eccezione diventi attiva.

9.1.3 [Conditional] Il Data Protection Officer / Privacy Advisor deve fornire consulenza sulle eccezioni formative in REG12 prima dell'approvazione quando l'eccezione incide su trattamenti ad alto rischio, PII di categorie particolari, gestione dei diritti, gestione degli incidenti, trasferimenti internazionali o evidenze di certificazione.

9.1.4 [Conditional] Top Management deve approvare in REG12 le eccezioni alla formazione privacy prima dell'attivazione quando l'eccezione incide su mancato completamento ripetuto, accesso privilegiato ai PII, trattamento di PII ad alto impatto o evidenze rivolte alle autorità di regolamentazione.

9.1.5 [All] Il Privacy Lead / PIMS Manager deve definire in REG12 il proprietario dell'eccezione, la data di scadenza, l'azione compensativa e la data di riesame prima di approvare qualsiasi eccezione alla formazione privacy.

9.1.6 [All] Il Process Owner / Business Owner deve chiudere o rinnovare in REG12 le eccezioni approvate alla formazione privacy prima della data di scadenza dell'eccezione.

10. Applicazione della politica

10.1.1 [All] Il Privacy Lead / PIMS Manager deve registrare in REG12 una non conformità formativa entro cinque giorni lavorativi quando le evidenze della formazione privacy obbligatoria sono mancanti, incomplete, scadute o non tracciabili in REG11.

10.1.2 [All] Il Process Owner / Business Owner deve assicurare che la formazione privacy obbligatoria scaduta sia completata o oggetto di escalation in REG11 o REG12 entro 10 giorni lavorativi dalla registrazione dello stato di scadenza superata.

10.1.3 [Conditional] Il System Owner / Application Owner deve limitare in REG12 i nuovi accessi PII ad alto impatto quando la formazione privacy richiesta in fase di onboarding o basata sui ruoli resta incompleta dopo l'escalation.

10.1.4 [Processor] Il Vendor / Procurement Owner deve gestire l'escalation delle evidenze mancanti di assurance della formazione di responsabili del trattamento, sub-responsabili o forza lavoro esterna in REG08 e REG12 entro cinque giorni lavorativi dall'identificazione.

10.1.5 [Conditional] L'Incident Response Coordinator deve collegare a REG10 le azioni di applicazione relative alla formazione entro un giorno lavorativo quando il fallimento formativo ha contribuito a un incidente relativo ai PII sospetto o confermato.

10.1.6 [All] L'Internal Audit / Compliance Reviewer deve verificare le evidenze di chiusura delle azioni correttive relative alla formazione in REG12 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] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica e i contenuti formativi almeno annualmente e registrare l'esito del riesame in REG11 o REG12.

11.1.2 [All] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica entro 30 giorni da una modifica sostanziale dell'ambito di applicazione del PIMS, della normativa privacy, delle attività di trattamento, del modello dei ruoli, delle lezioni derivanti da incidenti, delle risultanze dell'audit o dei risultati di efficacia della formazione.

11.1.3 [Conditional] Il Data Protection Officer / Privacy Advisor deve riesaminare in REG12 le modifiche della politica rilevanti ai fini privacy 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 aggiornare in REG11 i contenuti formativi e le evidenze di assegnazione entro 30 giorni da una modifica sostanziale approvata della 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 sui ruoli, le responsabilità e la 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 PII09 - Politica di raccolta, uso, comunicazione e condivisione dei PII;

12.11 PII10 - Politica di conservazione, cancellazione ed eliminazione dei 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 dei PII e controllo degli accessi;

12.15 PII15 - Politica di gestione degli incidenti e delle violazioni dei PII;

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

12.17 PII18 - Politica di monitoraggio, audit e miglioramento del PIMS.

13. Standard e quadri di riferimento

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].