					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII05					Titolo del documento: **Politica di gestione del consenso e delle preferenze**							
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	Informazioni documentate e controllo operativo per le evidenze del consenso
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoraggio, non conformità, azione correttiva e miglioramento
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Supporting	Collegamento alla base giuridica
ISO/IEC 27701:2025	Annex A.1.2.4; Annex A.1.2.5	Controller	Primary	Determinazione, acquisizione e registrazione del consenso
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registrazioni dei trattamenti del titolare del trattamento
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Accordi del responsabile del trattamento, finalità del cliente e registrazioni del responsabile del trattamento
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Supporto del responsabile del trattamento agli obblighi del titolare del trattamento verso gli interessati
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Protezione delle registrazioni del trattamento di PII
GDPR	Article 4(11)	Controller	Supporting	Criteri del consenso
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Liceità, correttezza, trasparenza e responsabilizzazione
GDPR	Article 6(1)(a); Article 6(4)	Controller	Primary	Consenso come base giuridica e collegamento al cambio di finalità

GDPR	Article 7	Controller	Primary	Condizioni del consenso e revoca
GDPR	Article 8	Conditional	Supporting	Escalation per il consenso dei minori
GDPR	Article 9(2)(a)	Conditional	Supporting	Consenso esplicito per il trattamento di categorie particolari
GDPR	Article 24	Controller	Supporting	Responsabilità e misure del titolare del trattamento
GDPR	Article 28	Both	Supporting	Collegamento a istruzioni e assistenza del responsabile del trattamento
GDPR	Article 30	Both	Supporting	Collegamento alle registrazioni dei trattamenti
ISO/IEC 29100:2020	Clause 5.2; Clause 5.8; Clause 5.12	Both	Supporting	Principi di consenso e scelta, trasparenza e conformità
ISO/IEC 29151:2022	Annex A.3	Both	Supporting	Controlli relativi a consenso e scelta
ISO/IEC TS 27560:2023	Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4	Conditional	Supporting	Struttura della registrazione e della ricevuta del consenso, ove utilizzate

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti obbligatori per determinare quando il consenso è richiesto, richiedere il consenso, acquisire le evidenze del consenso, gestire le preferenze, trattare le revoche, mantenere le registrazioni del consenso e riesaminare i meccanismi di consenso.

1.2 La presente politica si applica al trattamento di PII quando il consenso è scelto o richiesto come base giuridica, quando è richiesto il consenso esplicito, quando sono acquisite preferenze relative al consenso, oppure quando l'organizzazione gestisce registrazioni del consenso per conto di un titolare del trattamento.

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

1.4 Gli obblighi del responsabile del trattamento e del sub-responsabile si applicano solo quando registrazioni del consenso, stati delle preferenze o istruzioni di revoca del consenso sono gestiti in base a istruzioni documentate del titolare del trattamento o del cliente.

1.5 La presente politica non rende il consenso la base giuridica predefinita per il trattamento di PII.

1.6 La determinazione della base giuridica resta disciplinata da PII03 - Politica sull'inventario dei trattamenti di PII e sulla base giuridica.

2. Finalità

2.1 La finalità della presente politica è assicurare che la gestione del consenso e delle preferenze sia lecita, trasparente, dimostrabile, revocabile, tecnicamente applicabile e supportata da evidenze controllate.

2.2 La presente politica assicura che il consenso sia richiesto solo quando appropriato, che le registrazioni del consenso siano complete e tracciabili, che le revoche siano rispettate e che le evidenze del consenso restino disponibili per finalità di audit, richiesta di informazioni e responsabilizzazione.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 Assicurare che il consenso sia utilizzato solo quando è la base giuridica appropriata o quando è richiesto per l'attività di trattamento.

3.1.2 Assicurare che le richieste di consenso siano specifiche, informate, distinguibili e collegate all'informativa privacy applicabile.

3.1.3 Assicurare che le registrazioni del consenso e delle preferenze siano acquisite e mantenute in REG05.

3.1.4 Assicurare che le revoche e le modifiche delle preferenze siano gestite entro tempistiche operative definite.

3.1.5 Assicurare che le registrazioni del consenso siano collegate alle finalità del trattamento in REG02 e alle versioni dell'informativa in REG07.

3.1.6 Assicurare che le attività di supporto al consenso svolte da responsabili del trattamento e sub-responsabili seguano istruzioni documentate del titolare del trattamento o del cliente.

3.1.7 Assicurare che i meccanismi di consenso siano monitorati, riesaminati, corretti e verificabili mediante audit.

4. Dichiarazioni della politica

4.1 Applicabilità del consenso e base giuridica

4.1.1 [Controller] The Process Owner / Business Owner DEVE registrare in REG02 se il consenso è richiesto o scelto prima dell'avvio di qualsiasi nuova attività di trattamento di PII, o attività modificata in modo sostanziale, che si basi sul consenso.

4.1.2 [Controller] The Privacy Lead / PIMS Manager DEVE verificare in REG02 e REG05 che il consenso non sia scelto come base giuridica predefinita prima di approvare una nuova attività di trattamento basata sul consenso o modificata in modo sostanziale.

4.1.3 [Controller] The Data Protection Officer / Privacy Advisor DEVE riesaminare la base del consenso in REG04 prima del lancio quando il trattamento riguarda categorie particolari di PII, servizi rivolti a minori, trattamenti ad alto rischio o uno squilibrio tra l'organizzazione e l'interessato.

4.1.4 [Joint Controller] The Privacy Lead / PIMS Manager DEVE documentare in REG02 e REG05 la parte responsabile dell'acquisizione, della registrazione, del rinnovo e del rispetto del consenso prima dell'avvio del trattamento in contitolarità.

4.1.5 [Processor] The Privacy Lead / PIMS Manager DEVE registrare in REG08 e REG05 le istruzioni del cliente relative all'acquisizione del consenso, alla gestione delle preferenze o al supporto alla revoca prima di implementare un meccanismo di consenso per conto di un titolare del trattamento.

4.1.6 [Subprocessor] The Vendor / Procurement Owner DEVE registrare in REG08 gli obblighi del sub-responsabile relativi al consenso prima che a un sub-responsabile sia consentito gestire registrazioni del consenso, stati delle preferenze o istruzioni di revoca del consenso.

4.2 Richiesta e acquisizione del consenso

4.2.1 [Controller] The Process Owner / Business Owner DEVE assicurare che ogni richiesta di consenso sia specifica per finalità e collegata alla versione dell'informativa privacy REG07 applicabile prima che la richiesta di consenso sia presentata a un interessato.

4.2.2 [Controller] The System Owner / Application Owner DEVE configurare i meccanismi di consenso in modo da richiedere un'azione affermativa prima dell'inizio del trattamento quando è richiesto il consenso esplicito o opt-in.

4.2.3 [Controller] The Process Owner / Business Owner DEVE registrare in REG05 il riferimento all'interessato, la finalità, la categoria di PII, il testo o la versione del consenso, la versione dell'informativa privacy, il canale di acquisizione, la marcatura temporale, il metodo, lo stato e il periodo di validità applicabile quando il consenso è acquisito.

4.2.4 [Conditional] The Privacy Lead / PIMS Manager DEVE registrare in REG05 la logica di verifica dell'età o di autorizzazione e attivare il riesame REG04 prima del lancio quando il consenso riguarda trattamenti rivolti a minori.

4.2.5 [Conditional] The Privacy Lead / PIMS Manager DEVE contrassegnare il consenso come esplicito in REG05 prima dell'inizio del trattamento quando per la finalità selezionata è richiesto il consenso esplicito.

4.2.6 [Both] The System Owner / Application Owner DEVE impedire che il trattamento basato sul consenso prosegua prima che REG05 mostri uno stato di consenso attivo per la finalità pertinente.

[... 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] The Process Owner / Business Owner DEVE richiedere un'eccezione in REG12 prima di discostarsi da un requisito approvato relativo all'acquisizione del consenso, alla gestione delle preferenze, alla revoca o alle evidenze.

9.1.2 [All] The Privacy Lead / PIMS Manager DEVE approvare o respingere ogni eccezione relativa al consenso in REG12 prima dell'implementazione e assegnare una data di scadenza e un controllo compensativo per qualsiasi eccezione approvata.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor DEVE riesaminare l'eccezione in REG04 o REG12 prima dell'approvazione quando l'eccezione riguarda il consenso esplicito, trattamenti rivolti a minori, trattamenti ad alto rischio o un meccanismo di revoca.

9.1.4 [Both] The System Owner / Application Owner DEVE bloccare il rilascio in produzione o disabilitare il meccanismo di consenso interessato quando un'eccezione richiesta dalla presente politica non è stata approvata in REG12 prima della messa in esercizio.

10. Applicazione della politica

10.1.1 [All] The Privacy Lead / PIMS Manager DEVE registrare una non conformità relativa al consenso in REG12 entro cinque giorni lavorativi dall'identificazione di evidenze del consenso mancanti, non valide, non collegate o non affidabili.

10.1.2 [Controller] The Process Owner / Business Owner DEVE sospendere o porre rimedio al trattamento per la finalità interessata prima che prosegua qualsiasi ulteriore trattamento basato sul consenso quando il consenso è richiesto ma non può essere dimostrato in REG05.

10.1.3 [Both] The System Owner / Application Owner DEVE disabilitare o correggere un meccanismo di acquisizione del consenso, di preferenza o di revoca non conforme entro la tempistica assegnata in REG12.

10.1.4 [Processor] The Vendor / Procurement Owner DEVE segnalare tramite escalation in REG08 e REG12 le mancate esecuzioni delle istruzioni del cliente riguardanti registrazioni del consenso, stati delle preferenze o supporto alla revoca entro cinque giorni lavorativi dall'identificazione.

10.1.5 [All] The Internal Audit / Compliance Reviewer DEVE verificare le evidenze di chiusura delle azioni correttive relative al consenso in REG12 entro la data di scadenza assegnata.

11. Riesame e manutenzione

11.1.1 [All] The Privacy Lead / PIMS Manager DEVE riesaminare la presente politica annualmente e registrare l'esito del riesame in REG12.

11.1.2 [All] The Privacy Lead / PIMS Manager DEVE riesaminare la presente politica entro 30 giorni da una modifica sostanziale della normativa sul consenso, della tecnologia del consenso, degli strumenti di gestione delle preferenze, della struttura dell'informativa privacy o dei requisiti di certificazione PIMS.

11.1.3 [All] The Data Protection Officer / Privacy Advisor DEVE riesaminare in REG12 le modifiche alla presente politica significative per la 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] The Privacy Lead / PIMS Manager DEVE registrare in REG11 la comunicazione delle modifiche approvate alla 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 PII06 - Politica di gestione dei diritti dell'interessato

12.7 PII07 - Politica di valutazione del rischio privacy e DPIA

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

12.9 PII09 - Politica di raccolta, uso, divulgazione e condivisione di PII

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

12.11 PII11 - Politica di accuratezza e qualità di PII

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

12.13 PII14 - Politica di sicurezza e controllo degli accessi per PII

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

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

12.16 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.

13.2 La mappatura spiega in che modo la politica supporta i requisiti citati e identifica le clausole interne che li implementano o li supportano.

13.3 ISO/IEC 27701:2025

13.3.1 **Clause 7.5; Clause 8.1** - Mappato alle informazioni documentate e al controllo operativo per determinare l'applicabilità del consenso, acquisire le evidenze del consenso, gestire la revoca, versionare le registrazioni del consenso, testare i meccanismi e mantenere REG05. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.2; 4.5.3; 4.5.4; 7.1.1; 7.1.2; 7.1.3; 7.1.6].

13.3.2 **Clause 9.1; Clause 10.2** - Mappato al monitoraggio del consenso, alle metriche, al campionamento di audit, alla registrazione delle non conformità, alle azioni correttive e alla verifica dell'efficacia. Addressed by clauses [4.5.5; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.2; 10.1.3; 10.1.4; 10.1.5].

13.3.3 **Annex A.1.2.3** - Mappato alla conferma dei casi in cui il consenso è una base giuridica appropriata e al collegamento delle registrazioni del consenso alle registrazioni della base giuridica in REG02. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.2; 4.5.3].

13.3.4 **Annex A.1.2.4; Annex A.1.2.5** - Mappato alla determinazione di quando e come il consenso è ottenuto, all'acquisizione del consenso, alla registrazione della prova, alla gestione del consenso esplicito, della revoca, del rinnovo e dello stato del consenso. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.3.5 **Annex A.1.2.9** - Mappato alle registrazioni del titolare del trattamento per i trattamenti basati sul consenso, alla cronologia del consenso, al collegamento con l'informativa, alla conservazione delle evidenze e alle registrazioni del consenso disponibili per audit. Addressed by clauses [4.2.3; 4.3.6; 4.5.1; 4.5.3; 7.1.1; 8.1.1; 8.1.3].

13.3.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mappato agli accordi con i clienti del responsabile del trattamento, all'allineamento delle finalità e delle istruzioni del cliente e alle registrazioni del responsabile del trattamento quando sono svolti servizi di supporto al consenso per un titolare del trattamento. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 8.1.4; 10.1.4].

13.3.7 **Annex A.2.3.2** - Mappato al supporto del responsabile del trattamento agli obblighi del titolare del trattamento verso gli interessati quando la revoca del consenso, le modifiche delle preferenze o le evidenze del consenso sono gestite secondo le istruzioni del cliente. Addressed by clauses [4.3.4; 4.3.5; 4.5.4; 6.1.4; 8.1.4].

13.3.8 **Annex A.3.14** - Mappato alla protezione delle registrazioni del consenso e delle preferenze da alterazioni non autorizzate e alla conservazione delle evidenze della traccia di audit. Addressed by clauses [4.5.2; 5.1.6; 7.1.2; 10.1.5].

13.4 GDPR

13.4.1 **Article 4(11)** - Mappato ai criteri del consenso che richiedono che il consenso sia specifico, informato, affermativo ove richiesto e collegato alla finalità pertinente e alla versione dell'informativa. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.5].

13.4.2 **Article 5(1)(a); Article 5(2)** - Mappato a liceità, correttezza, trasparenza, evidenze di responsabilizzazione, campionamento di audit, azioni correttive e prova del trattamento basato sul consenso. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.5.3; 4.5.5; 8.1.1; 8.1.5; 10.1.1; 10.1.5].

13.4.3 **Article 6(1)(a); Article 6(4)** - Mappato al consenso come base giuridica per finalità specifiche e alla rivalutazione o al consenso rinnovato quando la finalità o le condizioni del trattamento cambiano in modo sostanziale. Addressed by clauses [4.1.1; 4.1.2; 4.4.1; 4.4.2; 4.5.3].

13.4.4 Article 7 - Mappato alla dimostrabilità, alle richieste di consenso distinguibili, alla revoca, alla facilità di revoca, alla validità del consenso e alla cronologia del consenso conservata. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.4; 4.4.5; 10.1.2].

13.4.5 Article 8 - Mappato all'escalation del consenso per servizi rivolti a minori, alla logica di verifica dell'età o di autorizzazione e al riesame del rischio privacy prima del lancio. Addressed by clauses [4.1.3; 4.2.4; 9.1.3].

13.4.6 **Article 9(2)(a)** - Mappato alla gestione del consenso esplicito quando il consenso esplicito è scelto per il trattamento di categorie particolari. Addressed by clauses [4.1.3; 4.2.5; 9.1.3].

13.4.7 **Article 24** - Mappato alle misure di governance del titolare del trattamento, al riesame, all'approvazione, alle eccezioni, alle azioni correttive e alla supervisione della direzione sui controlli del consenso. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.2; 6.1.3; 9.1.1; 9.1.2; 11.1.1; 11.1.4].

13.4.8 **Article 28** - Mappato alla gestione delle istruzioni del responsabile del trattamento, alle evidenze del supporto al consenso, al supporto alla revoca, agli obblighi del sub-responsabile e all'escalation delle istruzioni del cliente. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 10.1.4].

13.4.9 **Article 30** - Mappato al collegamento delle registrazioni del consenso alle finalità del trattamento, alle registrazioni del titolare del trattamento, alle registrazioni di supporto del responsabile del trattamento e alla tracciabilità REG02/REG05. Addressed by clauses [4.1.1; 4.5.3; 4.5.4; 7.1.1; 8.1.1].

13.5 ISO/IEC 29100:2020

13.5.1 **Clause 5.2; Clause 5.8; Clause 5.12** - Mappato a consenso e scelta, trasparenza e collegamento all'informativa, revoca, responsabilizzazione ed evidenze di conformità privacy. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.5.3; 4.5.5; 8.1.1; 10.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3** - Mappato ai controlli relativi a consenso e scelta che richiedono consenso significativo, informato e inequivocabile, modifica delle preferenze e modifiche tempestive del trattamento a seguito di modifica o revoca del consenso. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.4.5].

13.7 ISO/IEC TS 27560:2023

13.7.1 **Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4** - Mappato ai concetti di registrazione e ricevuta del consenso, alla tenuta delle registrazioni del consenso, alla struttura della registrazione del consenso, allo stato del consenso, al collegamento alla versione dell'informativa, alla struttura della ricevuta e all'interpretazione della ricevuta del consenso

quando tali registrazioni o ricevute sono utilizzate. Addressed by clauses [4.2.3; 4.3.2; 4.3.6; 4.4.3; 4.4.4; 4.5.2; 4.5.3; 7.1.6].

13.8 Internal Requirements

13.8.1 Requisito interno - Le clausole che definiscono REG05 come oggetto di evidenza autorevole, l'approvazione di evidenze non standard, il blocco del rilascio operativo, la formazione, la manutenzione della politica e la comunicazione supportano la coerenza dell'implementazione ma non sono mappate direttamente a una singola clausola esterna. Addressed by clauses [4.5.1; 5.1.2; 7.1.5; 9.1.4; 11.1.2; 11.1.3; 11.1.5].