| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Inserire qui la denominazione dell'entità giuridica registrata | | | | | | | |
| Numero del documento:<br>PII07 | | | | | Titolo del documento:<br>**Politica di valutazione del rischio privacy e DPIA** | | | | | | | |
| Versione:<br>1.0 | | Data di entrata in vigore:<br>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 6.1.1 | Both | Primary | Rischi e opportunità del PIMS |
| ISO/IEC 27701:2025 | Clause 6.1.2 | Both | Primary | Valutazione del rischio privacy |
| ISO/IEC 27701:2025 | Clause 6.1.3 | Both | Primary | Trattamento del rischio privacy e collegamento alla SoA |
| ISO/IEC 27701:2025 | Clause 6.3 | Both | Supporting | Modifiche pianificate al PIMS e rivalutazione del rischio |
| ISO/IEC 27701:2025 | Clause 7.5 | Both | Primary | Informazioni documentate su rischio privacy e DPIA |
| ISO/IEC 27701:2025 | Clause 8.1 | Both | Supporting | Pianificazione operativa e controllo |
| ISO/IEC 27701:2025 | Clause 8.2 | Both | Primary | Valutazione operativa del rischio privacy |
| ISO/IEC 27701:2025 | Clause 8.3 | Both | Primary | Trattamento operativo del rischio privacy |
| ISO/IEC 27701:2025 | Clause 9.1 | Both | Supporting | Monitoraggio e misurazione del rischio privacy |
| ISO/IEC 27701:2025 | Clause 9.3 | Both | Supporting | Riesame della direzione del rischio privacy |
| ISO/IEC 27701:2025 | Clause 10.2 | Both | Supporting | Non conformità e azioni correttive relative al rischio |
| ISO/IEC 27701:2025 | Annex A.1.2.6 | Controller | Primary | Valutazione d’impatto sulla privacy |
| ISO/IEC 27701:2025 | Annex A.1.2.9 | Controller | Supporting | Registrazioni dei trattamenti a supporto della valutazione del rischio |

| | | | | |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Annex A.2.2.2 | Processor | Supporting | Accordo con il cliente del responsabile del trattamento e assistenza DPIA |
| ISO/IEC 27701:2025 | Annex A.2.2.6 | Processor | Supporting | Informazioni del responsabile del trattamento a supporto della conformità del cliente |
| GDPR | Article 5(2) | Controller | Supporting | Evidenze di responsabilizzazione |
| GDPR | Article 24 | Controller | Supporting | Responsabilità e misure del titolare del trattamento |
| GDPR | Article 25 | Controller | Supporting | Protezione dei dati fin dalla progettazione e per impostazione predefinita |
| GDPR | Article 28 | Both | Supporting | Assistenza del responsabile del trattamento e istruzioni |
| GDPR | Article 30 | Both | Supporting | Registrazioni dei trattamenti a supporto della DPIA |
| GDPR | Article 32 | Both | Supporting | Rischio di sicurezza e misure di protezione |
| GDPR | Article 35 | Controller | Primary | Valutazione d’impatto sulla protezione dei dati |
| GDPR | Article 36 | Controller | Primary | Consultazione preventiva |
| GDPR | Article 39 | Conditional | Supporting | Consulenza e monitoraggio del DPO ove applicabile |
| ISO/IEC 29100:2020 | Clause 4.7; Clause 5.11; Clause 5.12 | Both | Supporting | Controlli privacy, sicurezza delle informazioni e conformità privacy |
| ISO/IEC 29134:2020 | Clause 1; Clause 5.1; Clause 6.2; Clause 6.3 | Both | Primary | Ambito, benefici, trigger e |

| | | | | |
|---|---|---|---|---|
| | | | | preparazione della PIA |
| ISO/IEC 29151:2022 | Clause 4.1; Clause 4.2 | Both | Supporting | Programma di protezione delle PII e identificazione dei requisiti |
| ISO/IEC 27557:2022 | Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7 | Both | Supporting | Integrazione della gestione del rischio privacy organizzativo |

## 1. Ambito di applicazione

1.1 La presente politica definisce i requisiti per la valutazione del rischio privacy, lo screening DPIA, l'esecuzione della DPIA completa, il trattamento del rischio, l'accettazione del rischio residuo, la consultazione, il riesame e la gestione delle evidenze per il trattamento delle PII nell'ambito di applicazione del PIMS.

**1.2 La presente politica si applica a:**

1.2.1 attività di trattamento delle PII nuove o modificate in modo sostanziale;

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

1.2.3 sistemi, applicazioni, servizi, processi aziendali, fornitori, responsabili del trattamento, sub-responsabili, trasferimenti internazionali e accordi di condivisione dei dati che incidono sul trattamento delle PII;

1.2.4 evidenze relative al rischio privacy e alla DPIA mantenute in REG04 ed evidenze di supporto mantenute in REG02, REG03, REG08, REG09, REG10, REG11 e REG12.

1.3 La presente politica non sostituisce i controlli sull'inventario dei trattamenti, i controlli sull'informativa privacy, i controlli sul consenso, i controlli sui diritti degli interessati, i controlli di protezione dei dati fin dalla progettazione, i controlli sui fornitori, i controlli sui trasferimenti internazionali, i controlli di sicurezza delle PII, i controlli sugli incidenti, i controlli sulle informazioni documentate o i controlli di monitoraggio/audit/miglioramento. Tali requisiti sono definiti nelle politiche correlate elencate nella Sezione 12.

1.4 Ai fini della presente politica, per valutazione del rischio privacy si intende l'identificazione, l'analisi, la valutazione, il trattamento, il riesame e il monitoraggio documentati dei potenziali impatti negativi sulla privacy derivanti dal trattamento delle PII.

1.5 Ai fini della presente politica, per DPIA si intende una valutazione documentata utilizzata per il trattamento in qualità di titolare del trattamento che possa presentare un rischio elevato per gli interessati e che valuta necessità del trattamento, proporzionalità, rischi, misure di protezione, rischio residuo, necessità di consultazione e condizioni di approvazione.

1.6 Ai fini della presente politica, per rischio privacy residuo elevato si intende un rischio privacy che rimane al di sopra della soglia di accettazione approvata dopo il trattamento del rischio proposto o attuato.

1.7 Ai fini della presente politica, per modifica sostanziale si intende qualsiasi modifica che incida sull'ambito di applicazione del PIMS, sulla finalità del trattamento, sulla base giuridica, sulle categorie di PII, sulle categorie di interessati, sulla scala del trattamento, sulla tecnologia di trattamento, sul monitoraggio o sulla profilazione, sul processo decisionale automatizzato, sugli interessati vulnerabili, sui destinatari, sui responsabili del trattamento, sui sub-responsabili, sui trasferimenti internazionali, sulla conservazione, sui controlli di sicurezza, sul profilo di rischio, sulle istruzioni del cliente o sull'ambito di certificazione.

## 2. Finalità

2.1 La finalità della presente politica è garantire che i rischi privacy e gli obblighi di DPIA siano identificati, valutati, trattati, approvati, riesaminati e documentati tramite evidenze prima che il trattamento delle PII generi un rischio inaccettabile per gli interessati o per il PIMS.

2.2 La presente politica consente all'organizzazione di dimostrare una governance privacy basata sul rischio, la responsabilizzazione del titolare del trattamento in materia di DPIA, l'assistenza DPIA da parte del responsabile del trattamento, il trattamento documentato del rischio, l'approvazione del rischio residuo, il processo decisionale sulla consultazione preventiva e il miglioramento continuo dei controlli privacy.

## 3. Obiettivi

### 3.1 Gli obiettivi della presente politica sono:

3.1.1 definire i trigger obbligatori di screening del rischio privacy;

3.1.2 definire quando è richiesta una DPIA completa;

3.1.3 assicurare che le decisioni DPIA del titolare del trattamento siano documentate e riesaminabili;

3.1.4 assicurare che l'assistenza DPIA del responsabile del trattamento e del sub-responsabile sia documentata ove richiesta da istruzione o accordo del cliente;

3.1.5 assicurare che i rischi privacy siano valutati prima dell'avvio di trattamenti delle PII nuovi o modificati in modo sostanziale;

3.1.6 assicurare che i trattamenti del rischio privacy siano assegnati, attuati e verificati;

3.1.7 assicurare che i rischi privacy residui elevati siano sottoposti a escalation e approvati prima che il trattamento inizi o continui;

3.1.8 assicurare che le decisioni di consultazione preventiva siano documentate ove permanga un rischio residuo elevato;

3.1.9 assicurare che le evidenze relative al rischio privacy e alla DPIA siano mantenute in REG04 e collegate agli oggetti evidenza correlati;

3.1.10 evitare la creazione di registri separati di DPIA, rischi o consultazioni al di fuori di REG04.

## 4. Dichiarazioni della politica

### 4.1 Screening del rischio privacy

4.1.1 [Both] Il Process Owner / Business Owner deve avviare lo screening del rischio privacy in REG04 prima dell'inizio di un trattamento delle PII nuovo o modificato in modo sostanziale registrato in REG02.

4.1.2 [Both] Il Privacy Lead / PIMS Manager deve mantenere i criteri di screening del rischio privacy in REG04 prima dell'operatività iniziale del PIMS e successivamente con cadenza annuale.

4.1.3 [Controller] Il Process Owner / Business Owner deve completare lo screening DPIA in REG04 prima dell'inizio di un trattamento in qualità di titolare del trattamento che soddisfi i criteri di screening del rischio privacy.

4.1.4 [Processor] Il Vendor / Procurement Owner deve registrare i requisiti di assistenza DPIA del cliente in REG08 prima dell'inizio del trattamento in qualità di responsabile del trattamento ove l'accordo con il cliente o l'istruzione documentata richieda supporto DPIA.

4.1.5 [Both] Il System Owner / Application Owner deve fornire evidenze sulla progettazione del sistema, sugli accessi, sulla sicurezza, sulla registrazione e sui flussi di dati in REG04 prima dell'approvazione della valutazione del rischio privacy per sistemi nuovi o modificati in modo sostanziale che trattano PII.

4.1.6 [Both] Il Privacy Lead / PIMS Manager deve registrare l'esito dello screening e la motivazione della decisione sulla DPIA completa in REG04 prima che l'attività di trattamento proceda.

### 4.2 Trigger della DPIA e determinazione dei requisiti

4.2.1 [Controller] Il Privacy Lead / PIMS Manager deve richiedere una DPIA completa in REG04 prima dell'inizio di un trattamento in qualità di titolare del trattamento che possa presentare un rischio elevato.

4.2.2 [Controller] Il Process Owner / Business Owner deve sottoporre al Privacy Lead / PIMS Manager in REG04, prima dell'inizio del trattamento, i trattamenti che comportano larga scala,

monitoraggio sistematico, profilazione, decisioni automatizzate, PII di categorie particolari, dati relativi a condanne penali o reati, interessati vulnerabili, tecnologie innovative o trattamento modificato in modo sostanziale.

4.2.3 [Controller] Il Data Protection Officer / Privacy Advisor deve registrare il proprio parere in REG04 prima dell'approvazione della decisione sul requisito di DPIA completa per trattamenti ad alto rischio in qualità di titolare del trattamento.

4.2.4 [Both] Il Process Owner / Business Owner deve ripetere lo screening del rischio privacy in REG04 prima di utilizzare PII per una nuova finalità, aggiungere un nuovo destinatario, introdurre un nuovo responsabile del trattamento o sub-responsabile, modificare l'architettura del sistema o avviare un nuovo trasferimento internazionale.

4.2.5 [Processor] Il Privacy Lead / PIMS Manager deve documentare se è richiesto supporto DPIA da parte del responsabile del trattamento in REG08 entro 10 giorni lavorativi dalla ricezione di una richiesta di assistenza DPIA del cliente.

4.2.6 [Subprocessor] Il Vendor / Procurement Owner deve documentare i requisiti di assistenza DPIA a monte in REG08 prima dell'inizio del sub-trattamento ove il cliente a monte o l'accordo con il responsabile del trattamento richieda tale assistenza.

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

## 9. Eccezioni

### 9.1 Eccezioni relative al rischio privacy e alla DPIA

9.1.1 [All] Il Process Owner / Business Owner deve richiedere qualsiasi eccezione alla presente politica in REG12 prima che si verifichi lo scostamento.

9.1.2 [All] Il Privacy Lead / PIMS Manager deve valutare l'impatto privacy, legale, di certificazione, operativo e sugli interessati di ciascuna eccezione richiesta in REG04 o REG12 entro 10 giorni lavorativi dalla richiesta.

9.1.3 [All] Il Data Protection Officer / Privacy Advisor deve registrare il proprio parere in REG12 prima dell'approvazione di qualsiasi eccezione che incida su trattamento ad alto rischio, completamento della DPIA completa, consultazione preventiva, rischio privacy residuo elevato o assistenza DPIA del cliente.

9.1.4 [All] Top Management deve approvare in REG12 le eccezioni relative al rischio privacy o alla DPIA che incidono su trattamento ad alto rischio, ambito di certificazione, consultazione preventiva o rischio privacy residuo elevato non risolto prima che l'eccezione abbia effetto.

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 al rischio privacy o alla DPIA prima dell'approvazione.

9.1.6 [All] Il Process Owner / Business Owner deve chiudere o rivalutare ciascuna eccezione relativa al rischio privacy o alla DPIA in REG12 entro cinque giorni lavorativi dalla scadenza.

## 10. Applicazione della politica

### 10.1 Applicazione della politica per il rischio privacy e la DPIA

10.1.1 [All] Il Privacy Lead / PIMS Manager deve registrare come non conformità in REG12 le evidenze REG04 relative al rischio privacy o alla DPIA mancanti, inesatte, incomplete, scadute o non approvate entro cinque giorni lavorativi dall'identificazione.

10.1.2 [Controller] Il Process Owner / Business Owner deve sospendere i nuovi trattamenti ad alto rischio in qualità di titolare del trattamento quando le evidenze richieste di approvazione DPIA in REG04 mancano prima del lancio.

10.1.3 [Both] Il System Owner / Application Owner deve bloccare la messa in esercizio di sistemi che trattano PII quando le evidenze richieste di trattamento del rischio in REG04 mancano prima dell'approvazione della messa in esercizio.

10.1.4 [Both] Il Vendor / Procurement Owner deve bloccare l'onboarding di fornitori, responsabili del trattamento, sub-responsabili o accordi di condivisione dei dati quando le evidenze richieste in REG04 relative al rischio privacy o all'assistenza DPIA mancano prima dell'approvazione dell'accordo.

10.1.5 [All] Top Management deve riesaminare in REG12 le principali non conformità relative al rischio privacy o alla DPIA non risolte durante il riesame della direzione.

10.1.6 [All] Il Privacy Lead / PIMS Manager deve sottoporre a escalation a Top Management in REG12, entro cinque giorni lavorativi dalla seconda occorrenza in un periodo di 12 mesi, i ripetuti mancati rispetto delle scadenze di screening REG04, riesame DPIA o trattamento del rischio.

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

## 11. Riesame e mantenimento

### 11.1 Riesame e mantenimento della politica

11.1.1 [All] Il Privacy Lead / PIMS Manager deve riesaminare la presente politica in REG12 annualmente ed entro 30 giorni da una modifica sostanziale ai requisiti relativi a rischio privacy, DPIA, consultazione preventiva, assistenza del responsabile del trattamento o certificazione.

11.1.2 [All] Il Privacy Lead / PIMS Manager deve riesaminare annualmente in REG12 i criteri di screening REG04, i criteri trigger per la DPIA, i criteri di classificazione del rischio e i criteri di accettazione del rischio residuo.

11.1.3 [All] Il 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] Il Privacy Lead / PIMS Manager deve aggiornare REG03 e REG04 entro 15 giorni lavorativi dopo modifiche approvate della politica che alterano l'applicabilità dei controlli, i criteri di rischio o i requisiti di screening DPIA.

11.1.6 [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 privacy

12.4 PII03 - Politica sull'inventario dei trattamenti delle 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 PII08 - Politica di protezione dei dati fin dalla progettazione e per impostazione predefinita

12.9 PII09 - Politica di raccolta, uso, comunicazione e condivisione delle PII

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 e controllo degli accessi alle PII

12.15 PII15 - Politica di gestione degli incidenti e delle violazioni delle 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 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 6.1.1** - Mappata all'identificazione e alla pianificazione delle azioni per rischi e opportunità privacy mediante criteri di screening, soglie di rischio, escalation e input al riesame della direzione. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Mappata allo svolgimento dello screening del rischio privacy, della valutazione del rischio privacy, della classificazione del rischio, della rivalutazione e della valutazione dei trigger DPIA prima che proceda un trattamento nuovo o modificato in modo sostanziale. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Mappata alla pianificazione del trattamento del rischio privacy, agli aggiornamenti dell'applicabilità dei controlli, all'attuazione del trattamento, all'accettazione del rischio residuo e al collegamento alla SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Mappata alle modifiche pianificate del PIMS e del trattamento che attivano la rivalutazione del rischio privacy e il riesame della DPIA. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mappata alle informazioni documentate controllate per screening del rischio privacy, evidenze DPIA, trattamento del rischio, accettazione del rischio residuo, decisioni di consultazione preventiva, eccezioni, non conformità ed evidenze di riesame della politica. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Mappata all'operatività dei controlli sul rischio privacy e sulla DPIA prima di messa in esercizio, onboarding, approvazione del trattamento, chiusura del trattamento e collegamento alle azioni correttive. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Mappata alla valutazione operativa del rischio privacy per modifiche di trattamento nuove, modificate, relative a sistemi, fornitori, trasferimenti e derivanti da incidenti. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Mappata al trattamento operativo del rischio privacy, all'assegnazione del trattamento, all'attuazione del trattamento, all'escalation dei trattamenti scaduti e alla verifica dell'efficacia. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Mappata al monitoraggio e alla misurazione della copertura dello screening, dello stato delle DPIA, dei rischi aperti, delle azioni di trattamento scadute, delle azioni dei fornitori, delle azioni di trattamento della sicurezza, delle azioni di rivalutazione degli incidenti e delle risultanze di audit. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Mappata al riesame della direzione dei rischi privacy residui elevati, delle azioni di trattamento scadute, dello stato delle DPIA complete, delle decisioni di consultazione preventiva e delle principali eccezioni di rischio privacy. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mappata alle non conformità relative al rischio privacy e alla DPIA, alle eccezioni, all'apertura di azioni correttive, all'escalation e alla verifica dell'efficacia. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Mappata alla valutazione della necessità e, ove appropriato, all'attuazione della valutazione d'impatto sulla privacy per trattamenti nuovi o modificati in qualità di titolare del trattamento. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Mappata alle registrazioni dei trattamenti a supporto degli input della valutazione del rischio privacy e della DPIA, incluse finalità, categorie, sistemi, destinatari, trasferimenti e fornitori. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mappata agli accordi con il cliente del responsabile del trattamento e agli obblighi di assistenza DPIA del cliente. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Mappata alla fornitura da parte del responsabile del trattamento delle informazioni necessarie per la conformità del cliente, incluse l'assistenza DPIA e le evidenze di supporto al cliente. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

**13.3 GDPR**

13.3.1 **Article 5(2)** - Mappata alle evidenze di responsabilizzazione per screening DPIA, decisioni di DPIA completa, trattamento del rischio, accettazione del rischio residuo, decisioni di consultazione preventiva, eccezioni, risultanze di audit e azioni correttive. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Mappata alla responsabilità del titolare del trattamento per misure adeguate in base al rischio privacy, riesame del rischio residuo elevato, approvazione della direzione e mantenimento della politica. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Mappata alle evidenze di protezione dei dati fin dalla progettazione e per impostazione predefinita utilizzate nella valutazione del rischio e prima dell'approvazione della messa in esercizio. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mappata all'assistenza DPIA del responsabile del trattamento e del sub-responsabile, alla gestione delle istruzioni del cliente e alle evidenze di trattamento del rischio dei fornitori. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Mappata alle registrazioni dei trattamenti a supporto degli input della valutazione del rischio privacy e della DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mappata agli input di rischio di sicurezza delle PII, alla selezione delle misure di protezione, al trattamento del rischio di sicurezza e agli aggiornamenti dello stato dei controlli di sicurezza. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mappata allo screening DPIA, alla determinazione del requisito di DPIA completa, al contenuto della DPIA, al parere del DPO, al riesame e al blocco dei trattamenti ad alto rischio privi dell'approvazione DPIA richiesta. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Mappata al processo decisionale sulla consultazione preventiva, al parere del DPO, all'approvazione di Top Management e alle azioni di prosecuzione, sospensione, riprogettazione o consultazione ove permanga un rischio residuo elevato. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mappata al parere e al monitoraggio del Data Protection Officer / Privacy Advisor ove applicabile per decisioni DPIA, trattamenti ad alto rischio, consultazione preventiva e modifiche della politica. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Mappata all'identificazione dei controlli privacy, alle misure di sicurezza, alla conformità privacy, alle evidenze del rischio privacy, al monitoraggio e al riesame. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

**13.5 ISO/IEC 29134:2020**

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mappata all'ambito del processo PIA, ai benefici, alla determinazione dei trigger, alla preparazione, agli input della valutazione, alle evidenze degli stakeholder e alla struttura del report DPIA mantenuta in REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

**13.6 ISO/IEC 29151:2022**

13.6.1 **Clause 4.1; Clause 4.2** - Mappata ai requisiti del programma di protezione delle PII, all'identificazione dei requisiti di protezione delle PII, alla selezione dei controlli basata sul rischio e al collegamento al trattamento del rischio privacy. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

**13.7 ISO/IEC 27557:2022**

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Mappata ai principi organizzativi di rischio privacy, alla leadership, all'integrazione, alla valutazione del rischio, al trattamento del rischio, al monitoraggio e riesame, e alla registrazione e reporting. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].