10 LINEE GUIDA PER L'IMPLEMENTAZIONE DELLA PRIVACY BY DESIGN NEL SDLC

10.1 Introduzione e concetti base

10.1.1 Principi della Privacy

All'interno dalla ISO/IEC 29100:2011 sono descritti undici principi che indirizzano la progettazione, lo sviluppo e l'implementazione dei requisiti di protezione della privacy (10.1.4). Questi principi, sono anche un riferimento per quel che concerne il monitoraggio e la misurazione delle prestazioni del software e per gli aspetti del controllo dei programmi di gestione della privacy in un'organizzazione (vedere anche paragrafo 5.8.1 dell'*Allegato 4 - Linee Guida per la modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design).*

Principi	**Descrizione**
Consenso e scelta	Secondo questo principio, l'interessato deve poter scegliere se acconsentire o meno al trattamento dei propri dati personali (Consenso Informato). Aderire a questo principio significa fornire all'interessato - in maniera chiara, facilmente comprensibile, accessibile e conveniente - i meccanismi per esercitare la scelta e fornire il consenso in relazione al trattamento dei suoi dati personali al momento della raccolta, al primo utilizzo o non appena possibile.
Scopo legittimo e specifico	Il principio di legittimità e specificità dello scopo assicura che quest'ultimo sia conforme alla legge applicabile e si basi su una base giuridica ammissibile.
Limitazione della raccolta	Limita la raccolta dei dati personali a ciò che è strettamente necessario per gli scopi specificati.
Minimizzazione dei dati	Prevede la progettazione, l'implementazione e l'elaborazione dei dati, attraverso procedure o sistemi ICT, in modo da ridurre al minimo i dati personali che vengono elaborati e il numero di parti interessate dalla privacy.
Limitazione dell'utilizzo, conservazione e divulgazione	Limita l'utilizzo, la conservazione e la divulgazione (incluso il trasferimento) dei dati personali a scopi specifici, espliciti e legittimi del trattamento.
Precisione e qualità	Assicura che i dati personali elaborati siano accurati, completi, aggiornati (a meno che non vi sia una base legittima per mantenere dati obsoleti), e adeguati e pertinenti ai fini del trattamento.
Apertura, trasparenza e preavviso	Tale principio prevede di fornite informazioni chiare e facilmente accessibili sulle politiche stabilite dal titolare del trattamento e sulle procedure relative al trattamento dei dati personali.
Partecipazione individuale e accesso	Stabilisce che agli interessati sia data la possibilità di accedere e di rivedere i propri dati personali, a condizione che la loro identità sia

	autenticata con un livello adeguato di garanzia e che tale accesso non sia vietato dalla legge applicabile.
Responsabilizzazione	Stabilisce che siano documentate e comunicate in modo appropriato tutte le politiche, le procedure e le pratiche relative alla privacy. Prevede altresì l'assegnazione ad un individuo specifico all'interno dell'organizzazione del compito di attuare le politiche, le procedure e le best practice relative alla privacy.
Sicurezza delle informazioni	Stabilisce la protezione dei dati personali con controlli appropriati a livello operativo, funzionale e strategico. Al fine di garantire l'integrità, la riservatezza e la disponibilità dei dati personali e proteggerli dai rischi (quali l'accesso non autorizzato, la distruzione, l'utilizzo non consentito, la modifica, la divulgazione o la perdita in tutto il ciclo di vita dell'informazione).
Conformità alla privacy	Stabilisce di verificare e dimostrare che il trattamento rispetti la protezione dei dati e la tutela della privacy, attraverso requisiti specifici e mediante verifiche periodiche – anche attraverso il ricorso a revisori interni o esterni.

Tabella 5 - Principi generali della privacy

A seguire vengono illustrate quelle che sono considerate come migliori pratiche in cui è il titolare del trattamento che definisce lo scopo dei dati e l'incaricato del trattamento che lo attua, coerentemente con gli obblighi definiti nel GDPR.

LIMITAZIONE NELLA RACCOLTA

- Limitazione nella raccolta dei dati personali
  - Prima della raccolta di dati personali - ad esempio, quando si stipula un contratto con l'interessato - il titolare del trattamento deve ottenere il consenso preventivo e inequivocabile da parte dell'interessato o informare l'interessato della raccolta di suoi dati personali e delle finalità di utilizzo indicate in base alla normativa nazionale vigente.
  - Dal punto di vista del titolare del trattamento, il consenso è necessario soprattutto quando i dati personali vengono utilizzati in servizi commerciali. Tuttavia, nei casi di sicurezza e di servizi pubblici, può non essere necessario un consenso esplicito preliminare, anche se è probabile che il consenso implicito sia stato fornito nell'ambito dell'accordo contrattuale tra l'utente e il fornitore di servizi.
- Metodi di raccolta dei dati personali
  - Il titolare del trattamento non deve acquisire dati personali con mezzi fraudolenti o altri mezzi illeciti.
- Raccolta dati senza consenso
  - Le limitazioni alla raccolta dei dati non si applicano nei casi in cui il trattamento dei dati personali è disciplinato dalla normativa nazionale vigente. I titolari del trattamento dei dati dovrebbero raccogliere i dati senza il consenso, ad esempio se autorizzati da un'ordinanza giudiziaria nazionale o da uno strumento giuridico equipollente.
- Esclusione di quelle informazioni in grado di identificare un individuo dai dati raccolti

- Il responsabile del trattamento dei dati dovrebbe adottare le opportune misure per evitare di raccogliere dati dai quali una persona potrebbe essere identificata facendo riferimento ad una banca dati.

- Conferma del consenso da parte dell'interessato per la raccolta dei propri dati personali
  - Il titolare del trattamento dei dati deve adottare misure adeguate per ottenere la conferma sul consenso da parte dell'interessato alla raccolta dei propri dati.

QUALITA' DEI DATI

- Qualità dei dati raccolti
  - Il titolare del trattamento dei dati personali deve adoperarsi nel mantenere i dati personali esatti e aggiornati entro i limiti necessari per il raggiungimento degli scopi dell'utilizzo.

SPECIFICA DELLO SCOPO

- Specifica dello scopo d'uso
  - Nel trattare i dati personali, il titolare del trattamento deve specificare le finalità dell'utilizzo dei dati personali.
- Limitazioni al cambiamento dello scopo d'uso
  - Il titolare del trattamento dei dati non deve modificare le finalità d'uso al di fuori dell'ambito in cui le nuove finalità possono ragionevolmente essere considerate compatibili con quelle d'origine.
- La modifica delle finalità d'uso richiede il consenso preventivo
  - Prima che il titolare del trattamento dei dati modifichi le finalità d'uso che vanno oltre il campo di applicazione in cui le nuove finalità possono ragionevolmente essere considerate compatibili con le finalità di origine, deve informare l'interessato di tale modifica o ottenere un consenso preventivo e inequivocabile.

LIMITAZIONE NELL'USO DEI DATI

- Limitazione d'uso
  - Un responsabile del trattamento dei dati personali non deve trattare i dati personali, senza ottenere il consenso preventivo da parte dell'interessato, oltre quanto necessario per il raggiungimento delle finalità d'uso specificate.
- Restrizione della divulgazione a terze parti
  - Il titolare del trattamento non deve fornire dati personali a terzi senza ottenere il consenso preventivo da parte dell'interessato, tranne in casi molto limitati e ben definiti (ad esempio a seguito di richieste legali).
- Utilizzo senza consenso
  - Le disposizioni delle due specifiche precedenti non si applicano nei casi in cui il trattamento dei dati personali si basa su leggi nazionali vigenti. I titolari del trattamento dei dati dovrebbero concedere l'accesso ai dati solo alle autorità incaricate all'applicazione della legge, come autorizzato da un'ordinanza di un tribunale nazionale o da uno strumento giuridico equivalente.

MISURE DI SICUREZZA

- I dati personali devono essere protetti da adeguate misure di sicurezza contro rischi quali la perdita o l'accesso non autorizzato, la distruzione, l'uso, la modifica o la divulgazione dei dati.

APERTURA

- Dovrebbe esistere una politica generale di apertura nei riguardi di sviluppi, pratiche e politiche in materia di dati personali. Dovrebbero essere prontamente disponibili mezzi per stabilire l'esistenza e la natura dei dati personali e le principali finalità del loro utilizzo, nonché l'identità e la residenza abituale della persona che raccoglie i dati.

PARTECIPAZIONE INDIVIDUALE

- Un individuo può avere il diritto, tra gli altri, di:
  a) ottenere dal titolare del trattamento la conferma dell'esistenza o meno di dati che lo riguardano;
  b) di avergli comunicato i dati che lo riguardano:
     i) entro un termine ragionevole;
     ii) ad un onere, se del caso, non eccessivo;
     iii) in modo ragionevole;
     iv) in una forma per lui facilmente comprensibile;
  c) essere motivati nel caso in cui una richiesta presentata ai sensi dei punti a) e b) viene respinta e di essere in grado di contestare tale rifiuto;
  d) contestare i dati che lo riguardano e, se la contestazione è accolta, far cancellare, rettificare, completare o modificare i dati che lo riguardano.

RESPONSABILIZZAZIONE

- Il titolare del trattamento dei dati deve essere responsabile del rispetto delle misure che attuano i principi di cui sopra e di garantire che i responsabili del trattamento dei dati allo stesso modo si conformino.

EQUIVALENZA DI REGIME

- Il titolare del trattamento dei dati non dovrebbe trasferire dati personali al di fuori delle proprie frontiere, a meno che la destinazione non abbia un regime di privacy equivalente a quello di origine.

10.1.2 Obiettivi di protezione

Gli obiettivi di protezione mirano a fornire delle proprietà astratte, ossia indipendenti dal contesto per i sistemi IT. Nella sicurezza ICT la triade della riservatezza, dell'integrità e della disponibilità è stata ampiamente accettata. Sebbene siano state proposte diverse estensioni e perfezionamenti, questi obiettivi di protezione *core* sono rimasti stabili per decenni e sono serviti da base per molte metodologie di sicurezza ICT, (cfr. DR-3). A completamento di questi obiettivi di protezione della sicurezza, sono stati proposti tre obiettivi di protezione specifici per la privacy che approfonditi nella tabella che segue:

Obiettivo	**Descrizione**
Incollegabilità	Garantisce che i dati rilevanti per la privacy non possano essere collegati tra domini con scopo e contesto comuni. Ciò significa che i processi devono essere gestiti in modo tale che i dati rilevanti per la privacy non siano collegabili a qualsiasi altro insieme di dati rilevanti sulla privacy al di fuori del dominio.
La trasparenza	Garantisce che tutte le elaborazioni dei dati rilevanti per la privacy, comprese le impostazioni legali, tecniche e organizzative, possano essere comprese e ricostruite in qualsiasi momento. Le informazioni devono essere disponibili prima, durante e

	dopo l'elaborazione. Pertanto, la trasparenza deve riguardare non solo l'elaborazione effettiva, ma anche l'elaborazione pianificata (trasparenza ex ante) e il tempo trascorso dall'elaborazione per sapere cosa è successo esattamente (trasparenza ex post)
L'intervenibilità	Garantisce l'intervento in relazione a tutti i trattamenti di dati relativi alla privacy in corso o pianificati, in particolare da parte di coloro i cui dati vengono elaborati. L'obiettivo dell'intervenibilità è l'applicazione di misure correttive e controbilanci ove necessario. L'intervenibilità è legata ai principi relativi ai diritti degli individui, ad es. i diritti di rettifica e cancellazione dei dati, il diritto di revocare il consenso o il diritto di presentare un reclamo o di sollevare una controversia per ottenere il rimedio.

10.1.3 Privacy by design

10.1.3.1 Definizione della Privacy by design

La Privacy by Design (PbD) è definita come "un approccio olistico concettuale che può essere applicato - end-to-end - all'interno di un'organizzazione, includendo le sue tecnologie informatiche, le sue pratiche commerciali, i suoi processi, la progettazione fisica e le infrastrutture di rete" (cfr. DR-8). Secondo questa impostazione, l'utente dovrebbe essere considerato il centro di un sistema di protezione dei dati personali (per definizione, quindi il sistema è "user centric"). Qualsiasi progetto - sia strutturale, sia concettuale - andrebbe realizzato considerando, sin dalla fase di progettazione, la riservatezza e la protezione dei dati personali. La PbD comprende la seguente trilogia di applicazioni:

- Sistemi IT;
- Pratiche di business;
- Progettazione delle reti.

E' in questo contesto che si inserisce la necessità di prevedere l'ingegnerizzazione della privacy by design in ogni fase del ciclo di vita del software.

10.1.3.2 I sette principi della privacy by design

Principio	**Descrizione**
Proattivo non reattivo; Preventivo non correttivo	L'approccio di *Privacy by Design* (PbD) è caratterizzato da misure proattive piuttosto che reattive. Essa è diretta ad anticipare e previene gli eventi invasivi della privacy prima che accadano. PbD non attende che i rischi per la privacy si materializzino, né offre rimedi per la risoluzione delle infrazioni della privacy una volta che si sono verificati, in quanto è diretta ad impedire che si verifichino.
Privacy come impostazione predefinita	La *Privacy by Design* è diretta a garantire il massimo grado di privacy prevedendo che i dati personali siano automaticamente protetti in qualsiasi sistema IT o di business. Nessuna azione è richiesta da parte dei singoli per proteggere la loro privacy, in quanto è integrata nei sistemi per impostazione predefinita.
Privacy incorporata nel design	La *Privacy by Design* è incorporato nel design e nell'architettura dei sistemi IT e di business. Non è attuata successivamente ad un evento. Il risultato è che la privacy diventa una componente essenziale delle

	funzionalità principali. La privacy è parte integrante del sistema, senza diminuirne la funzionalità.
Funzionalità completa; somma positiva, non somma zero	La *Privacy by Design* cerca di tutelare tutti i legittimi interessi e gli obiettivi in un'ottica *win-win*, senza prevedere delle soluzioni a somma zero che includano degli inutili trade-off. *Privacy by Design* evita la pretesa di false dicotomie, come la sicurezza a discapito della privacy, in quanto dimostra che è possibile averle entrambe.
Sicurezza end-to-end - Protezione completa del ciclo di vita	La *Privacy by Design* che è stata incorporata in un sistema sin dal primo momento, si estende in modo sicuro durante l'intero ciclo di vita dei dati coinvolti: prevedendo robuste misure di sicurezza - essenziali per la privacy - dall'inizio alla fine di un ciclo di vita. Ciò garantisce che tutti i dati vengano conservati e distrutti – in modo sicuro e tempestivamente - alla fine del processo. Pertanto, la *Privacy by Design* garantisce una gestione delle informazioni sicura end-to-end.
Visibilità e trasparenza - Keep it Open	La *Privacy by Design* cerca di assicurare a tutti gli stakeholder che qualunque sia la pratica aziendale o la tecnologia coinvolta, essa opererà secondo le promesse e gli obiettivi dichiarati, anche assoggettandosi a verifiche indipendenti. Le sue componenti e le sue operazioni rimangono visibili e trasparenti, sia per gli utenti che per i fornitori.
Rispetto per la privacy degli utenti - Mantenerlo incentrato sull'utente	La *Privacy by Design* richiede ai progettisti e agli operatori di garantire gli interessi dei singoli, offrendo robuste misure di privacy per impostazione predefinita. Prevedendo degli avvisi appropriati e potenziando le opzioni user-friendly, pertanto garantendo l'impostazione user-centric.

Tabella 6 - I sette principi della Privacy by Design

Vedere anche il paragrafo 5.8.1.2 dell'*Allegato 4 - Linee Guida per la modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design.*

10.1.4 Data protection Impact Assessment

La progettazione di qualsiasi software che coinvolga il trattamento dei dati personali deve essere preceduta da un'identificazione dei requisiti di protezione per la privacy, in quanto dal trattamento o dall'elaborazione dei dati personali potrebbero derivare dei rischi. I rischi per la privacy negli applicativi software che comportano il trattamento dei dati personali, dovrebbero essere trattati prima della loro implementazione, ossia sin dalla fase di progettazione (*Engineering Privacy by Design*). Dovranno, quindi, essere analizzati i rischi collegati alle applicazioni software.

In linea con i requisiti di attuazione previsti dal Regolamento (UE) 679 del 2016 (cfr. DR-1), di seguito indicato come **GDPR**, qualora un trattamento dei dati personali possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, i titolari di quest'ultimo dovranno effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali o *Data Protection Impact Assessment*, di seguito indicata come "DPIA" (cfr. Art. 35 DR-1), quest'obbligo è applicabile anche al ciclo di vita del software.

Sulla base di quanto stabilito dal WP Art. 29 (cfr. DR-7), sarà necessario effettuare una valutazione della necessità di svolgere una DPIA, basandosi sulla mappa concettuale definita nella Figura 27**.**

In particolare, al fine di valutare se il trattamento - posto in essere all'interno di un'applicazione software - possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche (Cfr. ART. 35 DR-1) sarà necessario determinare se rientra tra quelli indicati nella Tabella 7- in cui sono descritte alcune tipologie di trattamento che obbligano il titolare a svolgere una Data Protection Impact Assessment DPIA.

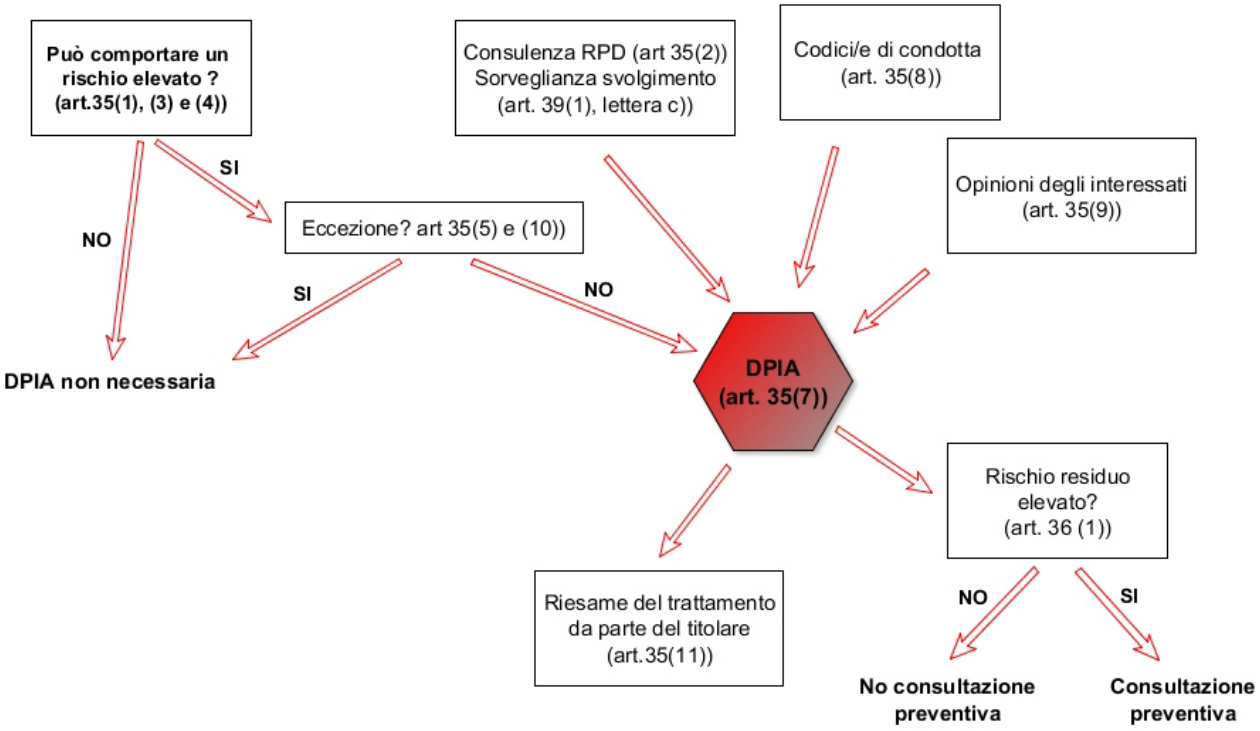

Figura 27 – Esempio di flusso di valutazione necessità DPIA

Alla luce di quanto sopra, se il trattamento, le sue modalità di attuazione o i dati trattati rientrano in quelli descritti nella Tabella 7, e non si configurano eccezioni – individuate all'interno di elenchi che dovranno essere redatti dagli Stati Membri (ad oggi non risultano essere stati ancora individuati) - sarà necessario svolgere una DPIA.

Tipologia di trattamento	Descrizione
1 - Valutazione di profilazione o scoring	Tutti quei trattamenti che analizzano i dati presenti all'interno dei propri archivi allo scopo di trarne informazioni riguardo il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato
2 - Decisioni automatizzate	Tutti quei trattamenti che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche
3 - Monitoraggio sistematico	Tutti quei trattamenti che sono utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza di

	un'area accessibile al pubblico
4 - Dati sensibili o estremamente personali	Tutti quei trattamenti che si riferiscono a particolari categorie di dati sensibili o estremamente personali
5 - Dati trattati su larga scala	Tutti i trattamenti che gestiscono dati personali su larga scala, in relazione al numero di soggetti interessati, al volume dei dati, alla durata o all'ambito geografico
6 - Combinazioni o raffronto di insieme di dati	Tutti quei trattamenti nei quali è prevista una presenza congiunta di due o più titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato
7 - Dati relativi a interessati vulnerabili	Tutti quei trattamenti in cui la tipologia delle informazioni trattate determina uno squilibrio fra interessato e titolare, nel senso della mancanza del potere, in capo al primo, di acconsentire o di opporsi al trattamento. Si inseriscono in questa categoria i dati dei minori, dei dipendenti o delle persone richiedenti specifiche tutele
8 - Utilizzi innovativi	Tutti quei trattamenti che utilizzano tecnologie o tecniche innovative per la raccolta o l'utilizzo dei dati personali, dato che il livello di conoscenza tecnologica, in un dato momento storico, non è in grado valutare il livello di rischio connesso all'innovazione
9 - Trattamenti che impediscono di esercitare un diritto o avvalersi di un servizio o contratto	Tutti quei trattamenti che impediscono agli interessati di esercitare un diritto di avvalersi di un servizio o di un contratto, ossia tutti i trattamenti dai quali l'interessato non può esimersi qualora volesse accedere a detto servizio o concludere detto contratto

Tabella 7 - Tipologie di trattamento che rappresentano un rischio elevato

Nel caso in cui la DPIA sia stata valutata come necessaria (cfr. DR-7), si potrà procedere con l'analisi degli impatti potenziali sui diritti e le libertà dell'interessato (persone fisiche), a fronte del trattamento dei relativi dati personali, allo scopo di porre in essere le opportune attività di trattamento dei rischi per la protezione dei dati personali.

In linea con quanto previsto da regolamenti e standard applicabili in materia (cfr. **Errore. L'origine riferimento non è stata trovata.**), tale attività costituisce un processo composto da un insieme di attività ben definite, da compiersi in sequenza ordinata, nell'ambito delle seguenti fasi:

1) **Definizione del contesto**, tramite la comprensione dell'organizzazione, dell'architettura tecnologica e dei fattori che potrebbero influenzare la gestione del rischio privacy;
2) **Privacy risk assessment**, attraverso cui si identificano, si analizzano e si valutano i rischi per gli interessati;
3) **Privacy risk treatment**, in cui si identificano le strategie e le modalità operative per l'implementazione delle misure di sicurezza adeguate alla copertura dei rischi rilevati in sede di risk assessment. (I requisiti di protezione per la privacy, da implementare all'interno del piano di trattamento dei rischi individuati per il software possono essere ricavati dai controlli descritti nella ISO/IEC 29151 (cfr. DR-5)

10.1.4.1 Riconoscere le informazioni personali

Per poter definire adeguatamente il trattamento del rischio privacy per i software, sarà necessario individuare le tipologie di informazioni personali, ossia quelle da cui possono essere ricavati dei dati personali, che potrebbero essere trattate da un applicativo software. Per determinare se una persona fisica debba o meno essere considerata identificabile, sarà necessario prendere in considerazione diversi fattori. In particolare, si dovrebbe tenere conto dei mezzi che possono ragionevolmente essere utilizzati dai software per il trattamento dei dati personali. I software dovrebbero supportare meccanismi adeguati ad informare l'interessato, raccogliere il consenso e proteggere i suoi dati personali. Le seguenti specificazioni forniscono degli ulteriori chiarimenti su come determinare se un'informazione possa essere considerata personale.

Identificativi

In alcuni casi, l'identificabilità dell'interessato potrebbe essere molto semplice (e.g. quando l'informazione contiene o è associata ad un identificatore che è usato per riferirsi o per comunicare con l'interessato). Le informazioni possono essere considerate personali almeno nei seguenti casi:

- se contiene o è associato a un identificatore che fa riferimento a una persona fisica (ad esempio, il codice fiscale);
- se contiene o è associato a un identificatore che può essere correlato a una persona fisica (ad esempio, numero del passaporto, numero di conto);
- se contiene o è associato a un identificatore che può essere utilizzato per stabilire una comunicazione con una persona fisica identificata (ad esempio, una posizione geografica precisa, un numero di telefono);
- se contiene un riferimento che collega i dati a uno degli identificatori di cui sopra.

Altre caratteristiche identificative

Le informazioni non devono necessariamente essere associate a un identificatore per poter essere considerate personali. Le informazioni saranno considerate personali anche se contengono o sono associate a una caratteristica che distingue una persona fisica da altre persone fisiche, ad esempio i dati biometrici. Qualsiasi attributo che assume un valore che identifica univocamente un l'interessato deve essere considerato come una caratteristica identificativa. Si noti che indipendentemente dal fatto che una determinata caratteristica distingue una persona fisica da altre potrebbe cambiare a seconda del contesto di utilizzo. Ad esempio, mentre il cognome di una persona fisica potrebbe essere insufficiente per identificare quella persona fisica su scala globale, potrebbe invece esserlo su una scala aziendale. Inoltre, potrebbero anche esservi situazioni in cui una persona fisica è identificabile anche se non esiste un singolo attributo che la identifica in modo univoco. Questo è il caso in cui una combinazione di diversi attributi messi insieme consente di distinguere tale persona dalle altre, ad esempio la combinazione degli attributi "femmina", "45" e "avvocato" può essere sufficiente per identificare una persona fisica all'interno di una determinata organizzazione, ma con buona probabilità sarà insufficiente per identificare quella persona fisica al di fuori di tale contesto.

La tabella che segue fornisce alcuni esempi di attributi che potrebbero essere personali, a seconda del dominio.

Età o bisogni speciali delle persone fisiche vulnerabili Accuse di condotta criminale Qualsiasi informazione raccolta durante i servizi sanitari Conto bancario o numero di carta di credito	Posizione derivata dai sistemi di telecomunicazione Storia medica Nome Identificativi nazionali (ad es. Numero di

Identificatore biometrico	passaporto)
Estratto conto della carta di credito	Indirizzo e-mail personale
Condanne penali o reati commessi	Numeri di identificazione personale (PIN) o password
Rapporti di indagini penali	Interessi personali derivati dall'utilizzo di tracciamento di siti Web
Numero cliente	Profilo personale o comportamentale
Data di nascita	Numero di telefono personale
Informazioni sanitarie diagnostiche	Fotografia o video identificabili con una persona fisica
Disabilità	Preferenze di prodotto e servizio
Fatture del medico	Origine razziale o etnica
Stipendi dei dipendenti e file di risorse umane	Credenze religiose o filosofiche
Profilo finanziario	Orientamento sessuale
Genere	Appartenenza sindacale
Posizione GPS	Bollette
Traiettorie GPS	
Indirizzo di casa	
Indirizzo IP	

Tabella 8 - Esempi di attributi per indentificare una persona

Dati pseudonimizzati

Al fine di limitare la capacità del titolare o del responsabile di identificare l'interessato, l'identità di quest'ultimo e le informazioni che lo riguardano possono essere sostituite da pseudonimi. Tale sostituzione viene solitamente eseguita da un soggetto terzo prima di trasmettere le informazioni a un destinatario. La sostituzione viene considerata pseudonimizzazione quando:

(a) gli attributi collegati allo pseudonimo non sono sufficienti per identificare l'interessato;

(b) l'assegnazione degli pseudonimi è tale da non poter essere invertita da parte delle persone che l'hanno eseguita.

La pseudonimizzazione evita il collegamento. Ma essendo diversi i dati collegabili allo stesso pseudonimo, esiste il rischio che la pseudonimizzazione sia violata, in quanto più grande è il set di dati associato a un dato pseudonimo, maggiore è il rischio che la proprietà (a) venga violata. Inoltre, più piccolo è il gruppo di persone fisiche a cui un insieme di dati pseudonimi si riferisce, maggiore sarà la probabilità che un interessato sia identificabile. Gli attributi contenuti direttamente nelle informazioni in questione e quelli che possono essere facilmente collegati a queste informazioni (ad es. utilizzando un motore di ricerca o dei riferimenti incrociati con altri database) devono essere presi in considerazione nel determinare se l'informazione si riferisce a un elemento identificabile dell'interessato.

La pseudonimizzazione è differente dall'anonimizzazione: i processi di anonimizzazione soddisfano entrambe le proprietà (a) e (b) di cui sopra, ma eliminano il collegamento. Durante l'anonimizzazione, le informazioni sull'identità vengono cancellate o sostituite da pseudonimi per i quali la funzione di associazione viene distrutta. Quindi, i dati resi anonimi non sono più personali.

Metadati

I dati personali possono essere memorizzati in un sistema ICT in modo tale da non essere facilmente visibili all'utente del sistema. Ad esempio, la memorizzazione del nome dell'interessato come metadato nelle proprietà di un documento, nei commenti o nelle modifiche. L'interessato deve essere a conoscenza dell'esistenza di tali dati sotto forma di metadati o del loro trattamento per tale scopo, in quanto potrebbe preferire che le informazioni personali non vengano elaborate in questo modo o condivise pubblicamente.

Dati non richiesti

Anche le informazioni personali non richieste da un titolare, cioè non intenzionalmente ottenute, potrebbero essere memorizzate da un software. Ad esempio, l'interessato potrebbe fornire delle informazioni personali anche quando non è stato richiesto dal trattamento (ad es. ulteriori informazioni personali fornite nel contesto di un modulo di feedback anonimo su un sito Web). Il rischio di raccogliere informazioni personali indesiderate può essere ridotto considerando le misure di tutela della privacy al momento della progettazione del software.

I dati personali stabiliti dal GDPR (cfr. **DR-1**) sono suddivisi nelle seguenti categorie di dati personali:

Categorie di dati personali	Descrizione
Dati identificativi	I dati identificativi rappresentano tutti quei dati che possono identificare, direttamente o indirettamente una persona, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online.
Dati Particolari/Sensibili	I dati particolari sono tutti quei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Dati giudiziari	I dati giudiziari rappresentano tutti quei dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

10.1.5 Flusso informativo del trattamento

Per definire l'architettura e il design di un software i progettisti dovranno prendere in considerazione la struttura del flusso informativo, descrivendo le interazioni tra interessato, titolare, responsabile e terze parti all'interno dell'applicativo software. Gli attori identificati possono interagire tra loro in vari modi, secondo i seguenti scenari, maturati dalla ISO/IEC 29134:2017[45]:

[45] https://www.iso.org/standard/62289.html

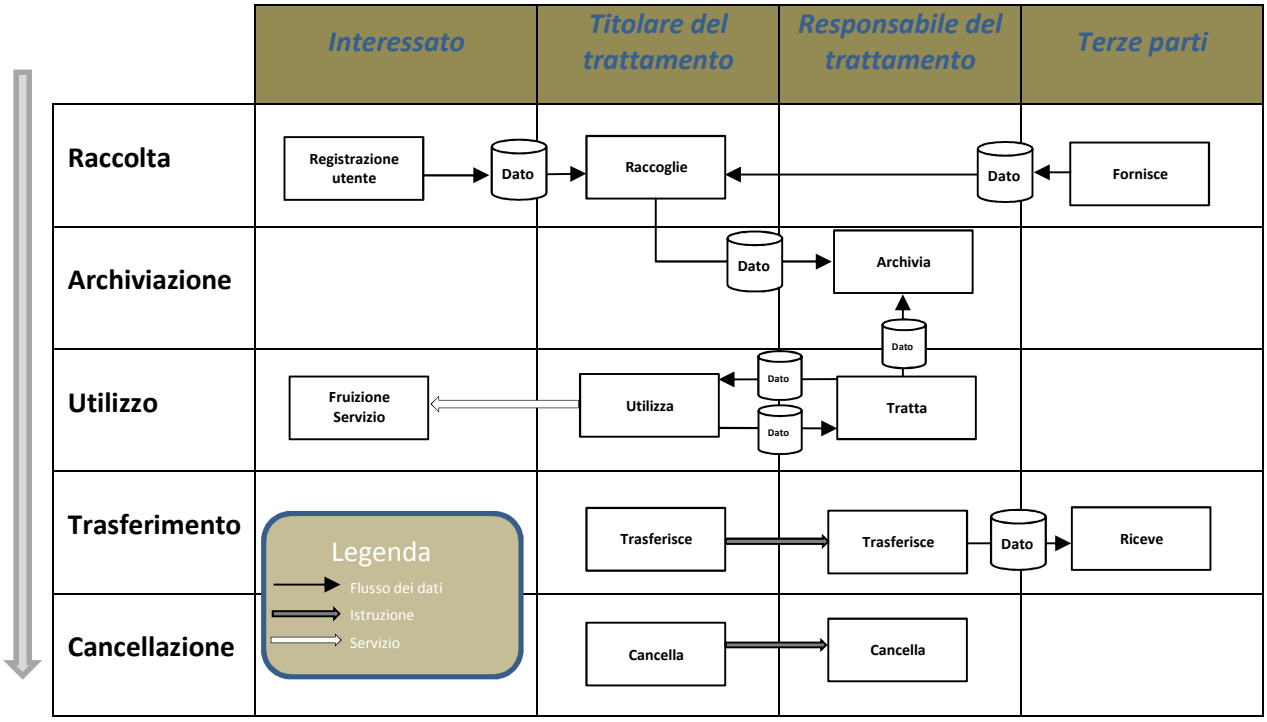

Figura 28 - Esempio di flusso informativo del trattamento

10.1.6 Privacy Implementation Strategy

La Privacy Implementation Strategy prevede che i progettisti del software definiscano e selezionino un modello di ciclo di vita adeguato all'ambiente di produzione e di sviluppo, all'ambito, all'ampiezza e alla complessità del progetto, parametrato sulle necessità emerse dai risultati della data protection impact assessment per la privacy (10.1.4).

Dovranno essere documentate:

- I principi generali della privacy applicabili alla progettazione del software (10.1.1)
- Gli obiettivi di protezione che il software dovrebbe garantire (10.1.2)
- I principi della privacy by design applicabili alla progettazione del software (10.1.3.2)
- I risultati della data protection impact assessment per il software e l'individuazione dei requisiti di protezione per la privacy (10.1.4)
- Le tipologie di Informazioni Personali Identificabili (PII) trattate nell'ambiente software (10.1.4.1)
- La descrizione del flusso informativo derivante dal trattamento all'interno del software (10.1.5)

10.2 Ciclo di vita dello sviluppo software nell'ambito del GDPR

Molti articoli che trattano la tecnologia dell'informazione sulla base del regolamento generale sulla protezione dei dati dell'UE si focalizzano su specifici obblighi commerciali e legali in materia di dati personali. Tali articoli si concentrano spesso sul trattamento fisico dei dati e sugli obblighi del responsabile di quest'ultimo nella gestione dello stesso. Questa è una considerazione importante per le organizzazioni che operano nell'UE.

Tuttavia, oltre alla localizzazione dei dati, il GDPR ha un impatto profondo e significativo sul ciclo di vita dello sviluppo del software e sui relativi processi di sviluppo informatico per quelle organizzazioni che prevedono la realizzazione di progetti relativi a sistemi informativi all'interno dell'UE.

Il reparto IT di un'organizzazione può utilizzare uno dei molteplici e distinti tipi di SDLC (System Development LifeCycle) presenti sul mercato, come Agile, DevOPS, Waterfall, Iterative e così via. Nonostante i nomi e gli approcci differenti, queste tipologie di SDLC hanno diverse aree in comune: tutti gli SDLC hanno una qualche forma di pianificazione, progettazione, realizzazione, test, rollout e mantenimento che coprono l'intero ciclo di vita di un sistema informativo.

Gli SDLC vengono utilizzati per costruire sistemi informatici gestendo e controllando con successo il progetto IT, sfruttando il fatto che la maggior parte dei sistemi informatici hanno livelli o moduli comuni.

In generale, nella maggior parte delle tecnologie impiegate, troviamo in comune i seguenti moduli:

- Livelli di trasporto dati e sicurezza;
- I livelli di database e architettura dei dati;
- I livelli applicativi e logici;
- I livelli di presentazione e portale.

L'SDLC, qualunque sia il tipo utilizzato, gestisce e controlla il progetto informatico, dalla pianificazione all'implementazione, attraverso i suddetti livelli o moduli.

Nell'ambito del GDPR vi è un numero significativo di requisiti e cambiamenti a livello di attività, processo, politica e procedure.

Il GDPR ha un impatto incredibile sul processo SDLC per quelle imprese che installano sistemi nell'UE e aumenta notevolmente la complessità dei progetti funzionali e tecnici associati ai vari livelli tecnici sopra descritti (ad esempio il livello di database).

I requisiti funzionali e tecnici introdotti dal GDPR per i sistemi informatici, sono sostanziali e non irrilevanti. In effetti, influenzano quasi tutti gli aspetti della progettazione e della realizzazione dei sistemi attraverso ciascuno dei suddetti livelli tecnologici. Tali influenze da parte del GDPR devono essere affrontate nella fase di pianificazione dell'SDLC, ovvero all'inizio, per evitare sovraccosti significativi e rielaborazioni successive nel processo informatico.

Segue un inventario di sedici aree di pertinenza ad articoli del GDPR che influenzano la pianificazione funzionale e tecnica dell'SDLC e i requisiti per i reparti IT. Tale elenco può essere considerato come un insieme di consigli generali per i CIO e i responsabili IT che redigono i requisiti dei loro sistemi operanti nell'ambito dell'UE:

1. L' implementazione della protezione dei dati nel sistema e nell'organizzazione, per progettazione e per impostazione predefinita, è un requisito legale:
    a. considerando 78 e Articolo 25
2. I dati devono essere protetti, e l'integrità e la riservatezza devono essere mantenute, utilizzando mezzi tecnici e organizzativi sotto la direzione del controllore:
    a. considerando 49 e Articoli 5-1(f), 32-1(b-d)
3. Ove possibile, deve essere utilizzata la cifratura dei dati:
    a. considerando 83 e Articoli 6-4(e), 32-1(a)
4. Ove possibile, deve essere utilizzata una pseudonimizzazione dei dati:
    a. considerando 26, 28, 29, 78 e Articoli 6-4(e), 25-1, 32-1(a)
5. Ove possibile, i dati devono essere resi anonimi:
    a. considerando 26
6. Al momento della raccolta dei dati, gli attributi del trattamento e le fasi elaborative devono essere forniti all'interessato, per via elettronica o per iscritto, in forma chiara e facilmente comprensibile:
    a. considerando 39, 58 e Articoli 12-1, 13-2(a-f)

7. Le persone interessate hanno il diritto di accedere ai loro dati e di controllarne il trattamento in qualsiasi momento:
    a. considerando 58, 61, 63 e Articoli 12, 15-1(a, d)
8. Separare le informazioni che potrebbero essere considerate dati personali o profili personali se trattati o combinati separatamente o insieme, al risultato di attività illecite:
    a. considerando 30
9. I dati relativi a un soggetto interessato dovranno essere portabili verso un altro provider (anche se concorrente):
    a. considerando 68 e Articoli 13-2(b), 14-2(c), 20
10. L'interessato ha diritto a una copia dei suoi dati in un formato comunemente utilizzato
    a. Articolo 15-3
11. L'interessato ha il diritto di ottenere gratuitamente l'aggiornamento dei propri dati in caso di errore.
    a. considerando 59, 65 e articolo 16 e, l'interessato ha il diritto di chiedere tale aggiornamento per via elettronica, riferimento 59
12. L'interessato ha il diritto di ottenere la cancellazione immediata dei dati che lo riguardano:
    a. considerando 59, 65 e articoli 13-2(b), 14-2(b), 17 e, l'interessato ha il diritto di chiedere tale cancellazione per via elettronica, riferimento 59 (Nota: Esistono nel GDPR particolari eccezioni a tale diritto.)
13. Il titolare del trattamento deve comunicare ad altre organizzazioni IT che detengono i dati dell'interessato che questi ha richiesto la cancellazione dei propri dati:
    a. considerando 66 e articolo 19 (quindi, il dipartimento IT deve sapere dove vengono conservati da terze parti tutti i dati degli interessati in modo che le parti coinvolte possano essere informate della richiesta di cancellazione. Sono essenziali inventari aggiornati dei dati interni ed esterni).
14. L'interessato ha il diritto di opporsi, revocare il consenso e rinunciare al trattamento. Questo può opporsi o revocare il proprio consenso in caso di trattamento elettronico dei propri dati:
    a. considerando 59, 63 e articoli 7-3,18,21 (e con raccomandazione tecnica del Consiglio UE: riferimento 67)
15. I dati vengono conservati solo per il tempo necessario a conseguire gli obiettivi dell'interessato. I dati personali scaduti non devono essere memorizzati. (Parte di una strategia di gestione dei registri elettronici). La persona interessata deve essere informata di tale periodo o delle modalità di elaborazione al momento della raccolta dei suoi dati:
    a. considerando 39, 45 e Articoli 13-2(a), 14-2(a), 25-2
16. Si deve stabilire, quasi immediatamente, se una violazione dei dati possa essere stata un "rischio elevato per i diritti e la libertà della persona fisica" in quanto deve essere predisposto l'opportuno ambiente tecnico per individuare, tracciare e valutare tali violazioni.
    a. considerando 85, 86 (relativi agli obblighi di notifica), 87 (Nota: Molti articoli, ad esempio 33,34) del GDPR riguardanti gli obblighi di comunicazione alla persona interessata e alle autorità competenti in materia.

Inoltre, molti dei punti di cui sopra, ad esempio l'undicesimo, richiedono aggiornamenti del contact center e interazioni e conferme con e da parte dell'interessato.

Una cosa è certa: ciascuno dei sedici punti di cui sopra dovrà avere una posizione nella documentazione di progettazione funzionale e tecnica dei sistemi realizzati con il supporto dell'SDLC, e ciascuno di essi apporterà una certa complessità alle fasi di progettazione del sistema nel suo complesso. In più, molti di questi influenzeranno anche i processi globali di assistenza verso i clienti dell'azienda, poiché il GDPR non

solo richiede determinati requisiti tecnici "puri", ma anche requisiti funzionali all'attività organizzativa supportati sia dalla tecnologia che dai processi aziendali.

In sintesi, il testo del GDPR contiene requisiti funzionali e tecnici del sistema, sia espliciti che impliciti, che influiscono e influenzano l'SDLC adottato dalle organizzazioni che progettano l'introduzione dei nuovi sistemi nell'UE.

L'impatto del GDPR sullo sviluppo del software inizia a partire dall'architettura dei dati e dai livelli di trasporto di questi, per arrivare fino ai livelli di portale e di presentazione. La chiave di base per il successo dello sviluppo IT è la pianificazione di tali requisiti durante le fasi iniziali dell'SDLC; sebbene possano aggiungere una certa complessità alle fasi iniziali di pianificazione e progettazione dell'SDLC, i costi di sviluppo complessivi saranno notevolmente ridotti al minimo se considerati il più precocemente possibile nel processo di costruzione dei sistemi IT.

10.3 Implementazione della strategia nelle fasi di sviluppo del software

10.3.1 Scopo

Gli elementi definiti all'interno della Privacy Implementation Strategy (10.1.6), i requisiti di protezione della privacy e le strategie di design per la privacy (ricavabili sulla base di quelli individuati da ENISA in DR-3), dovranno essere inquadrati all'interno di ciascuna fase della Engineering privacy by design (10.3.2) e rimappati per ciascuna fase del ciclo di vita dei software), così come definiti nelle fasi *Software life Cycle Processes* (cfr. DR-2).

10.3.2 Le fasi di implementazione della Engineering Privacy by Design

La seguente impostazione è stata maturata dal *Privacy Engineering Framework* del MITRE (cfr. DR-6), prevedendo le seguenti attività:

Attività	Descrizione
Definizione dei requisiti privacy:	Definizione delle proprietà della privacy di un software in modo che possa essere integrato con il design e lo sviluppo
Design e sviluppo privacy:	Definizione del design e sviluppo dei requisiti previsti
Verifica e validazione privacy:	Riscontro della conferma che i requisiti di privacy sono stati correttamente implementati e validati attraverso delle verifiche

Tabella 9 - Fasi dell'Engineering Privacy by Design

10.3.2.1 Definizione dei requisiti privacy

Input: Requisiti di privacy di base e test; Normative, best practice e procedure applicabili sulla privacy; requisiti funzionali; Profili di rischio per la privacy.

Attività: Svolgere una Data Protection Impact Assessment modernizzata sugli obiettivi di protezione individuati; Selezionare e perfezionare i requisiti di protezione per la privacy di base e effettuare dei test; Sviluppare dei requisiti di protezione della privacy personalizzati e testarli sulla base dei risultati della DPIA.

Output: Requisiti di protezione per la privacy specifici per il software.

10.3.2.2 Design e sviluppo privacy

Input: Requisiti Architetturali e funzionali specifici per la privacy

Attività: Identificare delle strategie e dei modelli di design della privacy; Identificare dei controlli di privacy, dei criteri tecnici e delle policy; Sviluppare dei dati e dei modelli di processo che riflettano i controlli di privacy identificati; Allineare, integrare e implementare i controlli di privacy con gli elementi funzionali; Analizzare il rischio del design di privacy complessivo (vedi anche Allegato 4 – Linee Guida per la modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design – Paragrafo 5.8).

Output: Componenti del software implementati; Mitigazione dei rischi accettabili per la privacy residua

10.3.2.3 Verifica e validazione privacy

Input: Componenti del software implementati; Requisiti di privacy specifici del sistema e test]; Politiche e procedure di privacy applicabili.

Attività: Sviluppare / perfezionare dei test sulla privacy; Eseguire delle verifiche sulla privacy; Verificare il comportamento operativo rispetto alle politiche e alle procedure sulla privacy applicabili.

Output: Risultati dei test di privacy; Documentazione delle Incoerenze sulla privacy documentate; Descrizione del piano di trattamento della privacy.

10.4 Integrazione della Engineering Privacy by Design nel Software Life Cycle Process

Il diagramma illustrato nella Figura 29, definisce la mappatura delle fasi della Engineering Privacy by Design sulle fasi del Software Life Cycle Process:

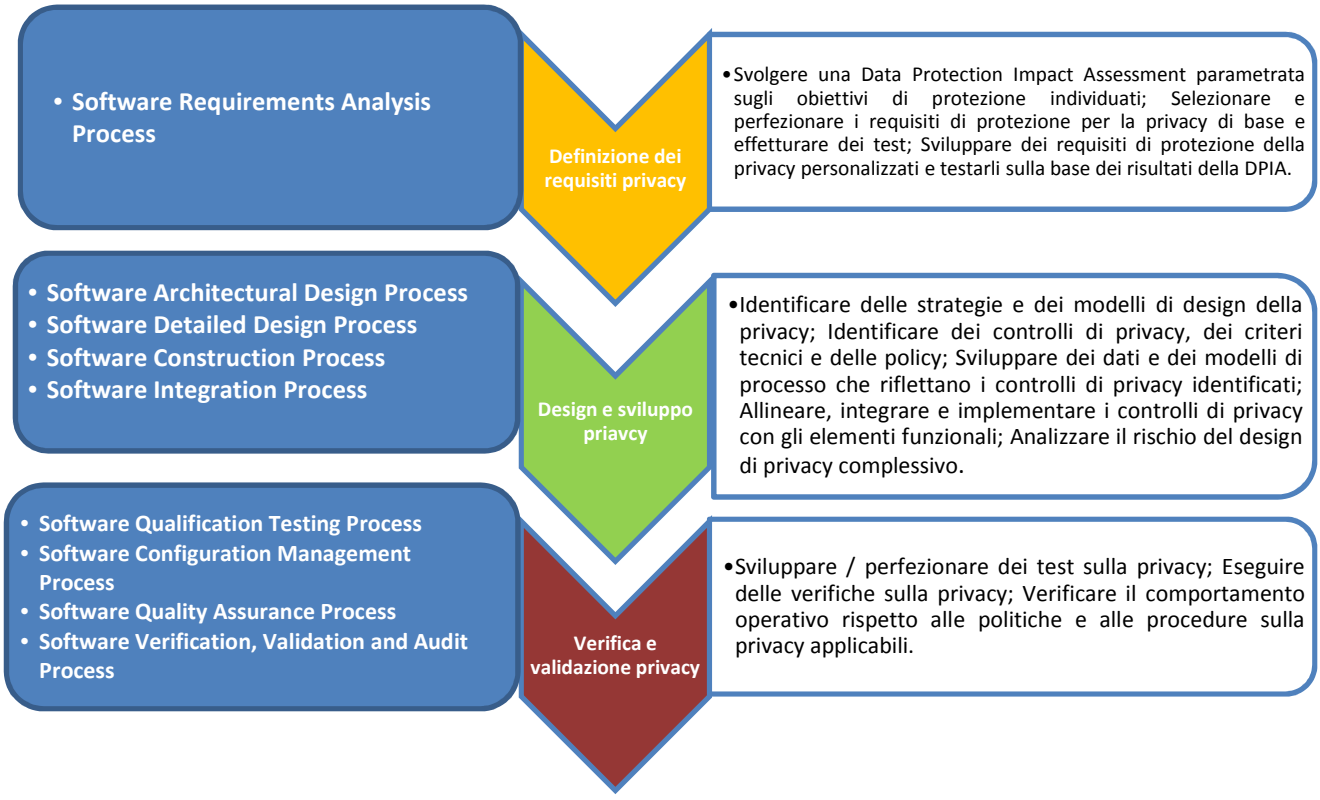

Figura 29 - Integrazione della Engineering privacy by design nel Software Life Cycle Process