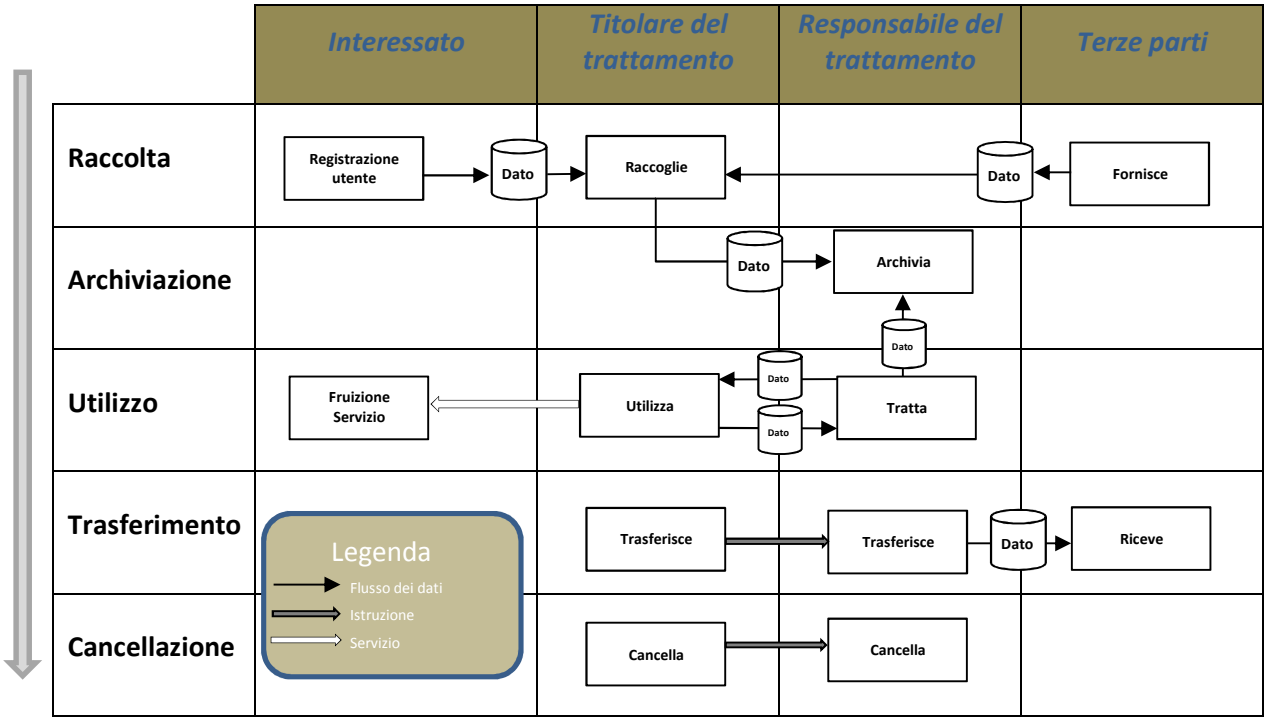

Figura 28 - Esempio di flusso informativo del trattamento

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