1. Contesto normativo.

Il GDPR disciplina il concetto di Privacy by Design all'art. 25 "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita". Ai sensi di tale disposizione, il Titolare del Trattamento ha il dovere di adottare misure tecniche e organizzative adeguate al fine di dare concreta attuazione alle disposizioni ed ai principi in materia di protezione dei dati (in particolare la *minimizzazione*), garantendo la conformità ai requisiti del regolamento ed un efficace esercizio dei diritti degli Interessati. A tale riguardo bisognerà tenere conto:

- dello stato dell'arte e costi di implementazione di ogni misura;
- della natura, contesto, ambito di applicazione e finalità del trattamento in progetto;
- dei rischi (e connessa probabilità e gravità degli stessi) che il trattamento potrebbe porre per le libertà e i diritti degli interessati;
- il progetto (applicazione o procedura organizzativa) che prevede l'istituzione e/o la modifica sostanziale di un trattamento, avendo come punto di riferimento il principio di "Privacy by Design", è da implementare in modo tale da porre particolare attenzione alla gestione dell'*intero ciclo di vita dei dati personali*, alla raccolta e alla cancellazione degli stessi con specifico riguardo alle garanzie procedurali in merito all'esattezza, alla riservatezza, all'integrità, alla sicurezza fisica e alla cancellazione dei dati personali.

Il GDPR, divenuto applicabile dal 25 maggio 2018, pone l'obbligo per il Titolare del Trattamento di dati personali di implementare:

- le misure tecniche e organizzative idonee ad attuare in modo efficace i principi di protezione dei dati e ad adottare nel trattamento le necessarie garanzie al fine di rispettare i requisiti del GDPR nonché tutelare i diritti degli interessati sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso (principio di "Privacy by Design");

- le misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, siano resi accessibili dati personali a un numero definito e limitato di persone fisiche (principio di "Privacy by Default").

Il Considerando n. 78 del GDPR prevede che il Titolare del trattamento dovrebbe adottare politiche interne nonché attuare misure che soddisfino in particolare i principi della protezione dei dati per impostazione predefinita sin dalla progettazione. Tali politiche dovrebbero concretizzarsi in specifiche misure volte a:

- ridurre al minimo il trattamento dei dati personali al fine di richiedere all'interessato esclusivamente quei dati strettamente necessari al perseguimento delle finalità individuate dal Titolare (c.d. principio di "minimizzazione");
- adottare un periodo di conservazione dei dati e di durata del trattamento tale da garantire che i dati non vengano conservati per un periodo superiore a quello strettamente necessario al perseguimento delle finalità previste o a quello imposto da eventuali obblighi di legge prevalenti;
- pseudonimizzare i dati personali o implementare le cautele più stringenti per la protezione dei dati per ciascuno specifico trattamento;
- garantire che il trattamento dei dati personali avvenga in piena trasparenza nei confronti dell'interessato mediante la descrizione esaustiva delle finalità e dei termini del trattamento all'interno di specifiche informative;

- consentire all'interessato di controllare il trattamento dei dati anche tramite l'esercizio dei diritti attribuiti agli Interessati dal GDPR;
- consentire al Titolare del Trattamento di adottare ed implementare i presidi di sicurezza destinati alla protezione dei dati personali.

2. Privacy by Design

Descrivere il processo che deve seguire ARS nel trattamento dei dati equivale a dare corpo ad uno dei principi portanti del GDPR, cioè quello della Privacy by Design e Privacy by Default che si sviluppa nei punti sotto riportati:

1. *Prevenire piuttosto che correggere*: l'approccio alla protezione dei dati personali deve mirare ad anticipare la nascita di un problema prima che si concretizzi anziché limitarsi a reagire una volta che il problema è insorto.
2. *Privacy come impostazione predefinita* (o "by Default"): occorre progettare ogni sistema in modo da garantire che, per impostazione predefinita, siano trattati esclusivamente i dati personali necessari a ogni specifica finalità del trattamento. Tale principio può essere declinato riducendo la quantità di dati raccolti, la portata del trattamento, il periodo di conservazione ed il numero di soggetti che hanno accesso ai dati personali.
3. *Privacy incorporata nella fase di progettazione* (o "by Design"): incorporazione della protezione dei dati nella progettazione di qualsiasi sistema, servizio, prodotto e pratica amministrativa. È necessario che la protezione dei dati diventi parte integrante delle funzioni di base di qualsiasi attività, sistema o servizio.
4. *Massima funzionalità* in presenza di condizioni di sicurezza: realizzazione di soluzioni tecnologiche con funzionalità non limitate dai presidi di sicurezza previsti dal progetto.
5. *Sicurezza fino alla fine*: piena protezione del ciclo vitale del prodotto o del servizio attraverso la messa in atto di efficaci misure di sicurezza sin dalla fase di progettazione del prodotto/servizio e durante tutto il "ciclo di vita dei dati". È necessario altresì adottare misure di elaborazione dei dati idonee, tali da prevedere la distruzione definitiva dei dati quando questi non siano più necessari o nel caso in cui si esaurisca il periodo di conservazione previsto e comunicato all'interessato.
6. *Corrispondenza fra i termini dichiarati all'interno dell'informativa con le caratteristiche del progetto di trattamento*: implementazione di soluzioni tecnologiche ed organizzative con funzioni che corrispondono, in modo fedele, alle informazioni fornite all'Interessato all'interno dell'informativa.
7. *Centralità dell'interessato*: progettazione di soluzioni tecnologiche ed organizzative che hanno come scopo primario la protezione delle libertà e i diritti degli interessati.

Premesso questo ci avviamo a descrivere il processo data protection, tenendo presente la suddivisione delle fasi relative ai controlli per la conformità all'interno del processo di definizione/modifica di un progetto il cui esito è reso dalla check list compilata, cui è seguita la verifica di conformità da parte del DP Specilist e le fasi successive che partono dall' identificazione dei requisiti della fornitura: se è previsto l'impiego di un fornitore esterno.

Il processo sarà descritto suddiviso nelle fasi necessarie e generali, ma non (generiche), affinché possa disciplinare attività eterogenee e sia adattabile sia alle attività scientifiche di ARS sia a quelle amministrative.

3. Conformità all'interno del processo di definizione/modifica di un progetto.

Il processo per la realizzazione o modifica di un progetto (processo di "demand/change") che prevede il trattamento di dati personali, può articolarsi nelle seguenti fasi:

3.*1 Raccolta delle esigenze*: il proponente si confronta con le funzioni competenti al fine di coordinare l'attività di individuazione e pianificazione delle iniziative organizzative ed informatiche (regolare rilevazione delle esigenze di servizi informatici e promozione delle opportunità tecnologiche offerte dall'evoluzione del sistema informativo). Sarà compito del proponente raccogliere e gestire le varie "esigenze" di servizi ICT avanzate dalle Funzioni competenti.

3.2 Valutazione delle esigenze: le varie esigenze raccolte dal proponente sono sottoposte al vaglio della Direzione, o funzione delegata, della società cui spetta il compito dell'analisi e valutazione. La Direzione affida la realizzazione del progetto ad un Responsabile in possesso delle competenze idonee per l'esecuzione dell'iniziativa.

3.3 Definizione preliminare del nuovo progetto: nel documento di definizione preliminare di progetto, elaborato, sia per i progetti interni (sviluppati interamente all'interno dell'agenzia) che per i progetti esterni (quelli commissionati ad un soggetto esterno), viene descritto il progetto costituito da una descrizione narrativa dei prodotti/servizi nonché delle finalità previste dal progetto.

3.4 Definizione dei requisiti del progetto (tra cui quelle relative alla sicurezza dei dati): prima di procedere con l'acquisizione o la realizzazione di una nuova soluzione tecnologica, il Responsabile effettua un'analisi (documentata) finalizzata alla descrizione dei requisiti del progetto, costituiti sia dalla descrizione dettagliata delle funzioni della soluzione tecnologica, sia dai presidi di sicurezza da impiegare per la protezione dei dati personali.

Comunicazione a Giunta e Consiglio delle attività non ricomprese nel programma di attività

Al fine di inserire le attività/progetti non ricomprese nel programma di attività nell'ambito delle finalità istituzionali dell'Agenzia della programmazione regionale, si provvede a darne comunicazione a Giunta e Consiglio (ex art. 82 bis, comma 2) fornendo la fotografia degli aspetti che caratterizzano l'attività e del collegamento alle aree tematiche individuate dagli indirizzi regionali, dalle funzioni e compiti di cui all'articolo 82 bis lr n. 40/2005 alla corrispondenza dell'attività ai trattamenti previsti dalla scheda n. 12 del regolamento regionale sulla protezione dati.

Il Responsabile definisce inoltre la scheda operativa necessaria per la realizzazione del progetto.

L'esecuzione di questa fase consente all'agenzia di minimizzare i costi di acquisizione e di realizzazione delle soluzioni e al contempo assicura che queste ultime siano in linea con l'indirizzo strategico e le finalità istituzionali di ARS che coinvolgono i processi amministrativi, le applicazioni, i dati, l'infrastruttura ed i servizi.

Il Responsabile coinvolge il DP Specialist, se necessario, ed esegue una valutazione dei rischi per le libertà e i diritti degli interessati considerando l'opportunità di adottare una o più misure di sicurezza utili alla mitigazione della probabilità di accadimento di minacce che possono colpire la riservatezza, l'integrità e la disponibilità dei dati personali trattati.

Allo scopo di verificare la conformità dei requisiti del progetto ai principi Privacy by Design / Default il DP Specialist, insieme alle funzioni competenti, compila una checklist (Checklist Privacy by Design / Default) che prevede:

- **Verifica indirizzi regionali:** l'art. 82 decies comma 1 della l.r. n. 40/2005 prevede che la Giunta regionale, recepite le indicazioni del Consiglio regionale, approvi specifici indirizzi per l'elaborazione del Programma di attività dell'Agenzia. Le attività devono trovare rispondenza rispetto alle aree strategiche individuate dalla Giunta.
- **Verifica finalità del trattamento:** ARS agisce quale soggetto titolare dei flussi amministrativi indicati nella scheda n. 12 del regolamento privacy di RT. Ha l'obiettivo di valutare e confrontare (tra gruppi di popolazione o tra strutture) l'appropriatezza, l'efficacia e l'efficienza dell'assistenza erogata, anche con riferimento a specifiche patologie o problematiche sanitarie e anche attraverso la caratterizzazione dell'esposizione a fattori di rischio, la ricostruzione dei percorsi diagnostici, terapeutici e assistenziali e l'analisi e il confronto degli esiti di salute. Occorre che la finalità dell'attività/progetto rientri nell'ambito delle finalità previste dalla scheda n. 12 quando si usano i flussi.

- **Verifica finalità istituzionale:** ARS si muove dentro i confini delineati dalla l.r. n. 40/2005: Occorre che le attività siano corrispondenti alle finalità indicate dall'articolo 82 bis. Le attività che non rientrano nell'ambito del l'articolo 82 bis, devono essere valutate appositamente e regolamentate da DPA specifici e da basi giuridiche diverse da quelle delle a legge regionale n. 40/2005 e dalla scheda 12 del regolamento regionale
- **Verifica dei Dati Personali**: il GDPR si applica esclusivamente ai dati che consentono, direttamente o indirettamente, di identificare delle persone fisiche (dati personali). Occorre anzitutto verificare quali dei dati da raccogliere possono definirsi come "personali", limitando la raccolta e il trattamento degli stessi esclusivamente a quelli realmente necessari alla realizzazione delle finalità perseguite, nel caso di dati anonimi, come quelli aggregati troverà applicazione il Considerando n. 26 del GDPR[1], che nel penultimo capoverso specifica la non applicazione del regolamento UE ai dati anonimi;
- **Verifica delle condizioni di liceità del trattamento**: le condizioni di liceità includono, tra l'altro, il consenso specifico e informato dell'interessato (ipotesi non frequente nell'attività dell'Agenzia), l'esecuzione di un contratto o lo svolgimento di trattative precontrattuali con lo stesso, la presenza di un obbligo legale cui è soggetto il Titolare del trattamento, l'esistenza di un legittimo interesse dello stesso Titolare o di terzi in assenza di prevalenti e confliggenti interessi o diritti o libertà fondamentali dell'interessato, la salvaguardia degli interessi vitali dell'interessato. Non è possibile eseguire attività di trattamento in assenza delle condizioni di liceità previste dal GDPR;
- **Determinazione del periodo di conservazione dei dati:** il Responsabile, consultati i responsabili delle funzioni competenti, stabilisce il periodo di conservazione dei dati in relazione alla finalità del trattamento in funzione dagli obblighi di conservazione stabiliti dalle norme vigenti (non solo in ambito privacy), considerando il principio di minimizzazione (Privacy by Default);
- **Valutazione della quantità dei dati personali raccolti**: il Responsabile, considerando i requisiti del progetto, comprensive delle funzioni da implementare, valuta se la quantità dei dati che saranno richiesti agli interessati, quantità intesa come numero delle informazioni richieste, è quella minima necessaria per l'esecuzione della finalità del trattamento nonché per l'esecuzione del servizio/progetto implementato;
- **Valutazione della portata del trattamento**: il Responsabile valuta se il target, inteso come numero e categoria di interessati i cui dati personali sono oggetto di trattamento, è ragionevolmente adeguato in funzione delle finalità del trattamento, anche in base ai requisiti del progetto e/o del prodotto;
- **Verifica dei privilegi di accesso al trattamento**: il Responsabile, al fine di rilevare il corretto rispetto delle caratteristiche tecniche per la riservatezza, volti a limitare l'accesso esclusivamente ai soggetti autorizzati preposti all'esecuzione del trattamento, determina a priori gli operatori che potranno accedere ai dati o alle applicazioni che gestiscono il trattamento degli stessi;
- **Verifica registro delle attività di trattamento**: il registro delle attività di trattamento è un adempimento che il GDPR pone in capo ai titolari e responsabili del trattamento e che consente di avere una chiara panoramica dei trattamenti di dati personali che vengono effettuati all'interno dell'organizzazione che fa per l'appunto capo al titolare o al responsabile. L'onere della tenuta del Registro è a carico del titolare o suo delegato e, se nominato, del responsabile del trattamento. La tenuta del registro è utile per una completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzata anche all'analisi del rischio di tali trattamenti e a una corretta pianificazione degli stessi. Il registro deve essere tenuto in forma scritta, anche in formato elettronico, e va esibito all'autorità di controllo in caso di verifiche.

[1] È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. **I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.** Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.

- **Verifica delle condizioni per l'esecuzione di un DPIA**: se il trattamento che si intende istituire, ricade fra quelli stabiliti dal Garante, o presenta almeno 2 (due) dei fattori indicati dal WP248, il Titolare deve necessariamente condurre una DPIA. Qualora l'esito della DPIA dovesse contenere Rischi Privacy Residui elevati, ritenuti dal Titolare "non accettabili", è prescritto dal GDPR l'interpello per la consultazione all'autorità di controllo[2].
- **Esito Controlli Privacy by Design/Default**: il DP Specialist, che ha condotto i controlli Privacy by Design, provvede alla segnalazione al Responsabile. La segnalazione può essere positiva o negativa. *Positiva*: se non sono rilevate criticità. *Negativa*: richiesta di integrazioni/segnalazioni errori/ segnalazione trattamenti illegittimi. La valutazione negativa non comporta il blocco del progetto, ma implica la responsabilità del Responsabile circa l'inosservanza della stessa, nel caso di successiva contestazione da parte degli interessati o dell'autorità di controllo. Se è stata effettuata la DPIA, la stessa sarà allegata al progetto.

3.5 Identificazione dei requisiti della fornitura.
Se è previsto l'impiego di un fornitore esterno sono definite le competenze che il fornitore deve garantire ed in particolare sono individuate le misure di sicurezza da adottare. Le caratteristiche definite in fase di progettazione, comprensive dei presidi di sicurezza, sono elementi utili alla definizione del servizio che il fornitore esterno dovrà erogare.

I requisiti del progetto costituiscono parte dei termini di negoziazione del contratto con il fornitore, definito ai sensi del GDPR, a seguito del perfezionamento dell'accordo, Responsabile del Trattamento.

3.6 Approvazione del progetto: il Responsabile approva e sottoscrive i requisiti del progetto. Il Responsabile propone la revisione del progetto per la correzione dei fattori critici emersi se necessario.

3.7 Attività preliminari all'implementazione progetto: il Responsabile conduce le operazioni preliminari per l'implementazione del progetto comprese quelle che dovranno essere implementate da fornitori esterni.

3.8 Committenza al fornitore: nel caso in cui sia previsto l'impiego di un fornitore esterno viene sottoscritto un contratto adeguato per la nomina come Responsabile del Trattamento (DPA –Data Protection Agreement- titolare-responsabile) con l'indicazione dei termini necessari al trattamento dei dati personali affidati. Laddove invece siano individuati ex GDPR i ruoli di titolari autonomi sarà utilizzato il DPA fra titolari autonomi che può essere sostituito da un apposito articolo da inserire nel corpo della convenzione/contratto.

3.9 Implementazione del progetto: il Responsabile, propone la revisione del progetto per la correzione dei fattori critici emersi se necessario; in assenza di fattori critici viene avviata la realizzazione del progetto sulla base delle caratteristiche in precedenza individuate.

Se il progetto che si intende implementare, presenta rischi elevati per le libertà e i diritti degli interessati, il titolare può decidere di interrompere e/o abbandonare l'implementazione dell'iniziativa.

[2] QUANDO LA DPIA E' OBBLIGATORIA?
In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto
(es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).
La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

3.10 Aggiornamento registro ed avvio del trattamento: il nuovo trattamento, o la variazione di un trattamento presente, viene registrato all'interno del registro dei trattamenti, indicando tutti gli elementi previsti dal GDPR.

A seguito dell'aggiornamento del registro è possibile eseguire le elaborazioni previste dal trattamento inerenti il progetto implementato.

3.11 Monitoraggio e controllo La direzione esegue, in accordo con le funzioni competenti (DP Specialist), controlli periodici al fine di verificare la corrispondenza delle misure di sicurezza individuate in sede di analisi Privacy by Design con quelle realmente applicate ai processi implementati ed in esecuzione. E' stato predisposto un apposito modulo per suddetto controllo.