

Check list da compilare quando viene formalizzata l'azione

Nome dell'azione (come da programma di attività):

Contatore (come da programma di attività):

Link alla pagina di PCG:

Nome e cognome del Responsabile:

Versione della check list:

Data:

Verifica	Lista da selezionare (se appropriato, la risposta può essere multipla)
<p>Verifica indirizzi regionali: L'art.82 decies comma 1 della l.r.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.</p>	<p><i>Indicazione aree strategiche:</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>epidemia Covid-19</i> <input type="checkbox"/> <i>disuguaglianze</i> <input type="checkbox"/> <i>ambiente e salute (prevenzione e promozione della salute)</i> <input type="checkbox"/> <i>valutazioni di impatto e di efficacia (politiche, attività, azioni, strumenti) ai fini della pianificazione, programmazione, organizzazione e supporto alla governance delle attività e dei servizi</i> <input type="checkbox"/> <i>modelli assistenziali (analisi, valutazione, modello di governance, valore prodotto) ai fini della pianificazione, programmazione,</i> <input type="checkbox"/> <i>organizzazione e supporto alla governance delle attività e dei servizi</i> <input type="checkbox"/> <i>azioni interne</i>
<p>Verifica finalità del trattamento: ARS agisce quale soggetto titolare dei flussi a: ministrativi 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.</p>	<p><i>Finalità del trattamento</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>programmazione dell'assistenza sanitaria</i> <input type="checkbox"/> <i>gestione dell'assistenza sanitaria</i> <input type="checkbox"/> <i>controllo dell'assistenza sanitaria</i> <input type="checkbox"/> <i>valutazione dell'assistenza sanitaria</i>
<p>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.</p> <p>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 della legge regionale n. 40/2005 e dalla scheda 12 del regolamento regionale.</p>	<p><i>Tipologia finalità:</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> <i>studi preparatori per gli atti di programmazione regionale;</i> <input type="checkbox"/> <i>definizione degli indicatori sullo stato di salute della popolazione e sui risultati delle attività del servizio sanitario regionale;</i> <input type="checkbox"/> <i>definizione strumenti per l'analisi dei bisogni sanitari e per l'analisi anche economica della domanda e dell'offerta delle prestazioni;</i> <input type="checkbox"/> <i>elaborazione di strumenti per la promozione e l'educazione alla salute al fine del miglioramento del quadro epidemiologico;</i> <input type="checkbox"/> <i>analisi e individuazione strumenti per verificare la qualità, l'equità di accesso e la rispondenza ai fini della</i>

	<p>salute dei cittadini dei servizi, delle prestazioni sanitarie e dei presidi farmaceutici, anche in funzione dell'attuazione del processo di accreditamento delle strutture sanitarie, previsto dal decreto delegato;</p> <p><input type="checkbox"/> circolazione delle conoscenze e dei risultati delle proprie attività di analisi e di ricerca.</p> <p><input type="checkbox"/> altro _____ (indicare)</p>
<p>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 , che nel penultimo capoverso specifica la non applicazione del regolamento UE ai dati anonimi.</p>	<p><i>Tipologia dati personali:</i></p> <p><input type="checkbox"/> dati anonimi,</p> <p><input type="checkbox"/> pseudonimizzati,</p> <p><input type="checkbox"/> personali in chiaro</p> <p><input type="checkbox"/> altro _____ (indicare)</p> <p><i>Indicare i flussi oggetto del trattamento:</i></p> <p>_____</p> <p>_____</p> <p>_____</p>
<p>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.</p>	<p><i>indicare la liceità di trattamento:</i></p> <p><input type="checkbox"/> obbligo di legge,</p> <p><input type="checkbox"/> consenso,</p> <p><input type="checkbox"/> adempimento di obblighi contrattuali,</p> <p><input type="checkbox"/> interessi vitali della persona interessata o di terzi, legittimo</p> <p><input type="checkbox"/> interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati</p> <p><input type="checkbox"/> interesse pubblico o esercizio di pubblici poteri</p>
<p>Verifica informativa</p>	<p><i>Indicare se è stata resa informativa (laddove necessaria)</i></p> <p>SI <input type="checkbox"/> NO <input type="checkbox"/> In corso di predisposizione <input type="checkbox"/></p>
<p>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).</p>	<p><i>indicare la durata della conservazione dei dati:</i></p> <p><input type="checkbox"/> durata del progetto</p> <p><input type="checkbox"/> 10 anni</p> <p><input type="checkbox"/> 5 anni</p> <p><input type="checkbox"/> illimitata</p>
<p>Valutazione dei dati personali raccolti: il Responsabile, considerando i requisiti del progetto, comprensive delle funzioni da</p>	<p><i>indicare:</i></p> <p>a) categorie degli interessati:(es: assistiti dal SSR, cittadini toscani, professionisti , titolari</p>

<p>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.</p>	<p><i>imprese, rappresentanti legali, personale dipendente ditte interessate, minori)</i> <i>b) tipologia del formato dei dati:</i> <input type="checkbox"/> <i>testo,</i> <input type="checkbox"/> <i>immagini</i> <input type="checkbox"/> <i>altro _____ (indicare)</i></p>
<p>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.</p>	<p><i>sottolineare se il trattamento dei dati è adeguato o non adeguato alla finalità del progetto</i></p>
<p>Individuazione ruoli GDPR e DPA: 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.</p>	<p><i>Indicare ruoli GDPR: (titolari, responsabili)</i> <input type="checkbox"/> <i>Titolari autonomi</i> <input type="checkbox"/> <i>Contitolari</i> <input type="checkbox"/> <i>Titolare / Responsabile</i> <i>In questo caso indicare i nomi:</i> <i>Titolare: _____</i> <i>Responsabile: _____</i> <i>Sub responsabile: : _____</i> <i>Indicare se è stato fatto DPA</i> <i>SI <input type="checkbox"/> NO <input type="checkbox"/> In corso di predisposizione <input type="checkbox"/></i></p>
<p>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.</p>	<p><i>indicare i nominativi dei soggetti autorizzati al trattamento dei dati relativi al progetto (da registro delle attività di trattamento)</i> <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____</p>
<p>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</p>	<p><i>E' stata censita l'attività nel registro delle attività di trattamento?</i> <i>SI <input type="checkbox"/> NO <input type="checkbox"/> In corso di predisposizione <input type="checkbox"/></i></p>

<p>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.</p>	
<p>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.</p>	<p><i>indicare se sussistono i seguenti fattori</i></p> <ul style="list-style-type: none"> - <i>trattamenti valutativi o di scoring, compresa la profilazione</i> SI <input type="checkbox"/> NO <input type="checkbox"/> - <i>decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni)</i> SI <input type="checkbox"/> NO <input type="checkbox"/> - <i>monitoraggio sistematico (es: videosorveglianza)</i> SI <input type="checkbox"/> NO <input type="checkbox"/> - <i>trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche)</i> SI <input type="checkbox"/> NO <input type="checkbox"/> - <i>trattamenti di dati personali su larga scala</i> SI <input type="checkbox"/> NO <input type="checkbox"/> - <i>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)</i> SI <input type="checkbox"/> NO <input type="checkbox"/> - <i>dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.)</i> SI <input type="checkbox"/> NO <input type="checkbox"/> - <i>utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.)</i> SI <input type="checkbox"/> NO <input type="checkbox"/> - <i>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)</i> SI <input type="checkbox"/> NO <input type="checkbox"/> <p><i>Indicare se è necessaria o no DPIA: SI <input type="checkbox"/> NO <input type="checkbox"/></i></p>

Parte a cura del DP Specialist	
<p>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.</p>	<p><i>VERIFICA</i> <i>(positiva/negativa)</i></p> <p><i>Note:</i></p>
	Data controllo: