

## LINEE GUIDA PER LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Allegato 2 del MOP  
Asl Sulcis Iglesiente

## NORMATIVA E DOCUMENTI DI RIFERIMENTO

- Reg. (UE) 2016/679 (GDPR) relativo alla protezione delle persone con riguardo al trattamento dei dati personali;
- D.lgs 10 agosto 2018, n. 101. “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- “Privacy Impact Assessment (PIA) Methodology”, Autorità francese per la protezione dei dati (CNIL), Febbraio 2018;
- “Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679”, WP 248 rev.01, 04/04/2017;
- “Linee guida sui responsabili della protezione dei dati”, WP 243 rev. 01, 05/04/17

▪

## INDICE

|   |        |
|---|--------|
| 1. OGGETTO E FINALITA'  | pag.3  |
| 2. DESCRIZIONE PROCEDURA  | pag.3  |
| 2.1. Ruoli e Responsabilità   | pag.3  |
| 2.2. Passi procedurali- Valutazione preliminare di necessità del DPIA | pag 3  |
| 2.3. Esecuzione del DPIA  | pag 4  |
| 2.3.1. Definizione del contesto                                       | pag. 4 |
| 2.4 Valutazione di necessità e proporzionalità del trattamento        | pag 5  |
| 2.5 Valutazione del rischio   | pag.5  |
| 2.5.1 Analisi degli impatti sui diritti e le libertà dell'interessato | pag.6  |
| 2.5.2 Analisi delle minacce applicabili                               | pag. 7 |
| 2.5.3. Valutazione del rischio effettivo                              | pag. 8 |
| 2.5.4 Definizione delle modalità di trattamento dei rischi            | pag.8  |
| 2.5.5. Redazione e approvazione del rapporto di DPIA                  | pag. 9 |
| 3. Attività conseguenti   | pag. 9 |
| 4. Revisione DPIA   | pag.10 |

## **1. OGGETTO E FINALITÀ**

Il Data Protection Impact Assessment (DPIA) o “Valutazione di impatto sulla protezione dei dati” rappresenta una delle fondamentali attività introdotte dal Regolamento UE 679/2016, di seguito sinteticamente indicato “GDPR”, relativamente agli obblighi dei Titolari (cfr. art 35), nell’ambito della gestione del rischio correlato al trattamento di dati personali.

La Valutazione d’Impatto sulla Protezione dei Dati è un processo strutturato volto a identificare e mitigare i rischi connessi al trattamento di dati personali, in particolare quando tale trattamento può comportare un rischio elevato per i diritti e le libertà degli interessati.

La DPIA è un adempimento essenziale per assicurare la conformità normativa e favorire un approccio proattivo alla protezione dei dati personali.

La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), oppure l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) o anche la mancata consultazione del Garante per la protezione dei dati personali laddove richiesto (articolo 36, paragrafo 3, lettera e), possono comportare sanzioni.

Scopo delle presenti Linee guida è quindi quello di dotare la Asl Sulcis Iglesiente di principi e metodologie comuni per lo svolgimento delle attività di valutazione d’impatto sulla protezione dei dati trattati, con definizione di responsabilità e ruoli nella relativa procedura

## **2. DESCRIZIONE PROCEDURA**

### **2.1. Ruoli e Responsabilità**

In fase di attivazione viene individuato un Responsabile, in genere il Process owner ossia il DESIGNATO del trattamento per l’esecuzione della DPIA, il quale sarà coadiuvato dall’Ufficio Privacy durante lo svolgimento e dovrà dare informazione al DPO circa l’attivazione della procedura stessa, il quale sorveglia lo svolgimento delle attività di DPIA al fine di rilevare eventuali difformità da quanto previsto dal Regolamento e/o dalle presenti linee guida e funge da punto di contatto con il Garante per la protezione dei dati personali in caso di consultazione preventiva di cui all'articolo 36 del GDPR.

Tutte le UO della Struttura Sanitaria, ognuno per il proprio ambito di competenza in relazione al trattamento, inclusa la UO che si occupa della gestione dei sistemi IT, supportano il titolare ed il DPO nello svolgimento delle valutazioni di impatto.

Qualora il trattamento venga eseguito in toto o in parte da un responsabile del trattamento dei dati, quest'ultimo deve assistere il titolare del trattamento nell'esecuzione del DPIA e fornire tutte le informazioni necessarie.

### **2.2 Passi procedurali- Valutazione preliminare di necessità del DPIA**

In base al Regolamento (art. 35) e alle specifiche fornite dal Garante, un DPIA è obbligatorio quando il trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

In particolare, il Regolamento prescrive la valutazione di impatto per i trattamenti che:

- Prevedono una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti

giuridici o incidono in modo analogo significativamente su dette persone fisiche;

- Prevedono il trattamento, su larga scala, di categorie particolari di dati personali (art. 9 GDPR) o di dati relativi a condanne penali e a reati (art. 10 GDPR);
- Prevedono la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Lo stesso Regolamento individua anche i seguenti casi per i quali non è invece obbligatorio eseguire un DPIA:

- a. Il trattamento appartiene ad una o più tipologie incluse in un elenco ufficiale di tipologie di trattamenti non soggetti al requisito di DPIA ai sensi del paragrafo 1 del art. 5 del GDPR, qualora pubblicato dall'autorità di controllo (Garante per la protezione dei dati personali);
- b. Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, par. 1, lettera c) o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1 lettera e), inoltre il trattamento trova nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare è soggetto una base giuridica, tale diritto disciplina il trattamento specifico o l'insieme di trattamenti in questione, ed è già stato effettuato un DPIA nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

Tutto ciò premesso, per determinare la necessità di eseguire un DPIA, devono adottarsi i seguenti criteri decisionali:

- Trattamenti che sottintendono un rischio elevato di violazione dei diritti e delle libertà delle persone fisiche (interessati);
- Trattamenti che non rientrano nei casi di cui ai precedenti punti a) e b) del precedente elenco;

### **2.3. Esecuzione del DPIA**

La valutazione d'impatto verrà effettuata dall'Azienda, come suggerito dal Garante, tramite il software messo a disposizione dal CNIL, l'applicativo PIA - Privacy Impact Assessment. al link <https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd>

Per l'esecuzione della DPIA si seguano le indicazioni fornite dai documenti di cui alla prima pagina "Normativa e documenti"

La fase di esecuzione del DPIA deve seguire i seguenti passi principali:

- Definizione del contesto;
- Valutazione di necessità e proporzionalità del trattamento;
- Valutazione dei rischi;
- Definizione delle modalità di trattamento dei rischi;
- Redazione e approvazione del rapporto di DPIA.

Durante l'esecuzione del DPIA l'Azienda può avvalersi di strumenti automatici o semi-automatici purché siano conformi alle presenti linee guida

#### **2.3.1. Definizione del contesto**

La definizione del contesto deve consentire una descrizione sistematica del trattamento oggetto della Valutazione di Impatto. Pertanto occorre individuare:

- Finalità del trattamento;
- Categoria di interessati (evidenziando se trattasi di minori);

- Responsabilità collegate al trattamento (titolare del trattamento, contitolare del trattamento, RDP, eventuali referenti interni, eventuali Enti terzi/Responsabili del trattamento);
- Gli asset a supporto del trattamento (strumenti, beni tecnologici e informatici usati quali applicativi/data base gestiti, PC, stampanti, reti locali, hardware, software, servizio in cloud, archivi ecc.).
- Categoria di dati personali trattati, ossia se si tratti di categorie particolari di dati personali (art. 9 GDPR), di dati personali relativi a condanne penali e reati (art. 10 GDPR), di dati sanitari biometrici genetici; di dati ultra-sensibili.
- Descrizione del flusso di dati identificando le principali operazioni di trattamento svolte, se l'informazione è soggetta a trasferimento verso paesi terzi o organizzazioni internazionali, ed in tal caso identificare il paese terzo o l'organizzazione internazionale e le condizioni per il trasferimento; se l'informazione è trattata all'interno di Fascicolo Sanitario Elettronico, Dossier Sanitario Elettronico e/o Referto on line; identificare i destinatari

Nello svolgimento di tale attività è necessario prendere come riferimento anche le informazioni contenute nel Registro dei Trattamenti predisposto dalla Amministrazione.

## **2.4 Valutazione di necessità e proporzionalità del trattamento**

Un punto fondamentale del DPIA è la descrizione delle modalità adottate per garantire la necessità e la proporzionalità del trattamento in relazione alle finalità.

In dettaglio, occorre:

- Illustrare perché le finalità del trattamento sono specifiche, esplicite e legittime;
- Presentare la base giuridica del trattamento, ossia se questa sia: il consenso dell'interessato, l'esecuzione di misure precontrattuali, l'esecuzione di un contratto, l'adempimento di obblighi legali del titolare, la salvaguardia di interessi vitali, l'esercizio di un interesse pubblico, legittimo interesse del titolare).

Se la base giuridica è il consenso occorre considerare e dimostrare che questo è:

- liberamente conferito, specifico, informato, inequivocabile e revocabile in qualunque momento;
- i dettagli del consenso sono stati registrati e che viene aggiornato in caso di modifiche

Se la base giuridica è il legittimo interesse del titolare occorre considerare e dimostrare che:

- non si applica nessun'altra base giuridica;
- il trattamento è necessario per raggiungere lo scopo, cioè non è possibile ottenere ragionevolmente lo stesso risultato in un altro modo meno invasivo;
- gli interessi, i diritti e le libertà dei singoli, non prevalgono sugli interessi dell'Amministrazione.

- Spiegare perché i dati raccolti sono necessari e quindi adeguati, rilevanti e limitati alle finalità del trattamento ("minimizzazione dei dati");
- Descrivere quali sono le misure adottate per assicurare l'accuratezza e l'aggiornamento dei dati;
- Spiegare perché la durata dell'archiviazione è giustificata da requisiti legali e/o necessità di trattamento.

## **2.5 Valutazione del rischio**

Nella fase di valutazione del rischio vanno identificate quali potenziali minacce possono riguardare gli interessati.

La valutazione dei rischi deve identificare gli “scenari di rischio” e, per ognuno di essi, stimare il “livello di rischio effettivo” per i diritti e le libertà dell’interessato connessi al trattamento in esame con riguardo alla natura, all’ambito di applicazione, al contesto e alle finalità del trattamento.

I principali scenari di rischio da prendere in considerazione sono:

- Perdita di riservatezza - accesso illegittimo ai dati personali;
- Perdita di integrità - modifica non autorizzata dei dati personali;
- Perdita di disponibilità - perdita, furto, cancellazione non autorizzata di dati personali.

Il livello di rischio è inteso come la probabilità che una minaccia possa sfruttare le vulnerabilità di un asset o di un gruppo di asset a supporto del trattamento e quindi causare un danno all’interessato.

La valutazione del livello di rischio deve pertanto essere stimato in termini di:

- “Impatto” potenziale sull’interessato nel caso in cui si concretizzi ognuno degli scenari di rischio e relativa probabilità di accadimento dello scenario di impatto;
- “Probabilità delle minacce” che dipende principalmente dal livello di vulnerabilità delle risorse di supporto e dalle minacce in grado di sfruttarle.

A tal fine la fase di valutazione del rischio deve prevedere le seguenti sotto-fasi:

- Analisi degli impatti sui diritti e le libertà dell’interessato e della probabilità di accadimento degli scenari di impatto;
- Analisi delle minacce applicabili al contesto di trattamento;
- Valutazione della probabilità di accadimento delle minacce identificate, in base al livello di implementazione dei controlli ed alla robustezza di questi ultimi nel contrastarle;
- Valutazione del rischio effettivo.

I principi per lo svolgimento delle suddette sotto-fasi sono dettagliati nei successivi paragrafi

### **2.5.1 Analisi degli impatti sui diritti e le libertà dell’interessato**

L’analisi degli impatti potenziali sui diritti e le libertà dell’interessato deve essere condotta considerando le seguenti dimensioni di analisi:

- Scenario di perdita di Riservatezza, Integrità e Disponibilità;
- Categoria di impatto.

Le categorie di impatto devono includere le seguenti:

- Impatto fisico: tutti i danni fisici che gli interessati potrebbero subire a seguito di violazioni dei dati personali;
- Impatto materiale: tutti i danni materiali che gli interessati potrebbero subire a seguito di violazioni dei dati personali;
- Impatto psicologico: tutti i danni psicologici che gli interessati potrebbero subire a seguito di violazioni dei dati personali.

Per ogni scenario e per ogni categoria occorre identificare un “livello di impatto”, espresso secondo una scala di valutazione qualitativa discreta (N.A.= Non Applicabile, 1=Trascurabile, 2=Limitato, 3=Significativo, 4=Massimo), descritta nella seguente tabella.

|         |                 | LIVELLI DI IMPATTO PER CATEGORIA   |   |   |
|---------|-----------------|--|---|---|
| Livello |                 | Impatto fisico   | Impatto materiale   | Impatto psicologico   |
| N.A.    | Non applicabile | Gli interessati non subirebbero alcun impatto.   | Gli interessati non subirebbero alcun impatto.  | Gli interessati non subirebbero alcun impatto.  |
| 1       | Trascurabile    | Gli interessati potrebbero incontrare qualche inconveniente fisico, superabile senza difficoltà (ad es. mal di testa).   | Gli interessati potrebbero incontrare qualche inconveniente materiale, superabile senza difficoltà (ad esempio perdita di tempo).   | Gli interessati potrebbero incontrare qualche inconveniente psicologico, superabile senza difficoltà (ad esempio semplice fastidio).  |
| 2       | Limitato        | Gli interessati potrebbero sperimentare inconvenienti fisici superabili nonostante alcune difficoltà (ad es. malattia lieve).  | Gli interessati potrebbero avere inconvenienti materiali, superabili nonostante alcune difficoltà (ad esempio: costi aggiuntivi o mancato accesso ad un servizio).                                | Gli interessati potrebbero avere inconvenienti psicologici, superabili nonostante alcune difficoltà (ad esempio disturbo psicologico minore ma oggettivo, intimidazione sui social network).  |
| 3       | Significativo   | Gli interessati potrebbero subire conseguenze fisiche significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà (ad esempio malattia a lungo termine). | Gli interessati potrebbero subire conseguenze materiali significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà (ad esempio perdita di opportunità non ricorrenti). | Gli interessati potrebbero subire conseguenze psicologiche significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà (ad esempio significativo disturbo psicologico, esposizione a ricatti, cyberbullismo). |
| 4       | Massimo         | Gli interessati potrebbero sperimentare gravi conseguenze fisiche, anche irrimediabili, che potrebbero non superare (ad esempio malattie permanenti o decesso).                    | Gli interessati potrebbero subire gravi conseguenze materiali, anche irrimediabili, che potrebbero non superare (ad esempio indebitamento ingente, impossibilità di lavorare).                    | Gli interessati potrebbero subire gravi conseguenze psicologiche, anche irrimediabili, che potrebbero non superare (ad esempio perdita di legami familiari, disturbo psicologico permanente o a lungo termine).                         |

Figura n. 1- Livello di impatto per categoria

Infine, occorre identificare gli scenari di impatto ritenuti probabili e definire i parametri di continuità del trattamento, da esprimere in termini di:

- Recovery Point Objective (RPO), inteso come massima quantità di informazioni (dati), in termini di elaborazione temporale, che è possibile perdere in caso di evento dannoso affinché l'impatto sia tollerabile;
- Recovery Time Objective (RTO), inteso come intervallo temporale massimo di indisponibilità, che si ritiene tollerabile in caso di evento dannoso.

### 2.5.2 Analisi delle minacce applicabili

L'analisi delle minacce deve essere basata su un "catalogo di minacce" derivanti da standard e best practices di riferimento, ognuna delle quali è caratterizzata da:

- Uno o più scenari di rischio che la minaccia può determinare (accesso illegittimo ai dati, modifica non autorizzata dei dati, perdita dei dati);
- La tipologia di asset sulla quale può agire;
- Uno o più agenti di minaccia che possono attuarla (fonti umane interne/esterne o fonti non umane).

Tra queste minacce occorre identificare quelle applicabili allo specifico trattamento in esame.

Per ogni minaccia identificata come applicabile al trattamento in esame, occorre valutare la probabilità di accadimento espressa su una scala di valutazione qualitativa discreta di 4 livelli (Trascurabile, Limitata, Significativa, Massima) prendendo in considerazione i tre scenari di rischio relativi alla perdita di riservatezza, integrità e disponibilità.

A tal fine, la probabilità viene derivata dal livello di attuazione dei controlli posti in essere a protezione del trattamento relativamente ai seguenti ambiti:

- Requisiti del Regolamento;
- Requisiti derivanti dalla normativa e dai pronunciamenti del Garante per la protezione dei dati personali;
- Requisiti derivanti da standard e best practices internazionali di sicurezza e privacy.

È opportuno che i controlli siano strutturati in “classi funzionali”, ciascuna delle quali individua funzionalità omogenee di sicurezza e privacy in grado di contrastare le minacce applicabili. Ogni controllo inoltre deve essere caratterizzato da un livello di robustezza su una scala ordinale a tre valori.

Per ogni controllo, il livello di implementazione “as is” dei controlli deve essere valutato, sia tramite intervista che autovalutazione, utilizzando la seguente nomenclatura convenzionale:

- “Sì”: il controllo è coperto da una o più contromisure pienamente e correttamente applicate (100%);
- “Parziale”: una o più contromisure coprono solo parzialmente il controllo espresso (più del 50% ma non ancora il 100%);
- “No”: il controllo non è coperto da alcuna contromisura oppure è solo parzialmente implementato (<50%);
- “N.A.”: il controllo non è applicabile al contesto di riferimento

### 2.5.3. Valutazione del rischio effettivo

Il rischio effettivo per i diritti e le libertà degli interessati connesso al trattamento in esame deve essere valutato per ogni scenario di rischio e per ogni minaccia, in base a:

- I valori di impatto rilevati, pesati con la probabilità degli scenari di impatto (cfr. par. 3.3.3.1);
- La probabilità di accadimento delle minacce.

I livelli di rischio rilevati devono essere espressi secondo una scala di valutazione qualitativa discreta a 4 livelli (1=Trascurabile, 2=Limitato, 3=Significativo, 4=Massimo), applicando i criteri espressi dalla matrice di rischio rappresentata nella figura seguente.

| IMPATTO | Trascurabile | Limitato | Significativo | Massimo |               |
|---------|--------------|----------|---------------|---------|---------------|
|         |              |          |               |         | Massimo       |
|         |              |          |               |         | Significativo |
|         |              |          |               |         | Limitato      |
|         |              |          |               |         | Trascurabile  |
|         | PROBABILITA' |          |               |         |               |

### 2.5.4 Definizione delle modalità di trattamento dei rischi

Una volta valutato il rischio effettivo, il titolare, identifica quale tra le seguenti opzioni per il trattamento del rischio ritiene di adottare:

- Evitare il rischio, rinunciando, ad esempio, alle attività che lo generano;



- Condividere il rischio con un'altra parte in grado di gestire il rischio in modo più efficace, come ad esempio assicuratori e fornitori;
- Ridurre il rischio ad un livello ritenuto accettabile, attraverso l'implementazione delle contromisure necessarie al raggiungimento di tale soglia;
- Accettare il rischio se non si ritiene opportuna alcuna delle precedenti opzioni.

In tal senso, la Struttura Sanitaria, nella persona del titolare, adotta, in funzione del livello di rischio effettivo riscontrato, l'approccio sintetizzato nella seguente tabella:

Quando il livello di rischio risulta essere Massimo o Significativo, è consigliabile prendere in considerazione:

- L'opzione evitare, in caso di gravi violazioni di legge o di pericolo per le incolumità delle persone;
  - L'opzione condividere, quando scartata l'opzione precedente, il costo di tale condivisione (in termini di tempi e costi) è minore di quello associato all'implementazione delle contromisure di sicurezza per la riduzione del rischio;
  - L'opzione ridurre, anche congiuntamente a quella di condividere, quando il titolare ritiene opportuno l'implementazione delle contromisure necessarie al raggiungimento di un livello di soglia ritenuto accettabile.
- Se la strategia di trattamento approvata prevede la riduzione, occorre valutare il livello di rischio residuo che si raggiungerà a valle della applicazione della strategia scelta ed i requisiti da attuare per il suo conseguimento, che saranno successivamente dettagliati all'interno di specifici piani di sicurezza. In base al livello di rischio residuo ed ai tempi previsti per il suo raggiungimento, il titolare valuta la necessità di consultare il Garante come dettagliato nel successivo paragrafo.

In ogni caso, a prescindere dal livello di rischio effettivo valutato, occorre definire una strategia di trattamento mirata a soddisfare tutti i requisiti normativi, non coperti o parzialmente coperti.

#### **2.5.5. Redazione e approvazione del rapporto di DPIA**

Come ultima attività del DPIA è prevista la redazione ed approvazione del rapporto di DPIA che deve contenere almeno i seguenti argomenti:

- La descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- La valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- I risultati della valutazione dei rischi per i diritti e le libertà degli interessati in linea con l'art. 5 par. 1 del Regolamento;
- Le misure previste per affrontare i rischi e dimostrare la conformità al Regolamento.

Il documento deve essere approvato dal titolare e riportare i nominativi di chi ha contribuito alla redazione ed alla revisione del documento (RDP, responsabili del trattamento, etc.).

Il titolare può prendere in considerazione, in taluni casi, la pubblicazione di alcune parti del rapporto di DPIA. Il documento pubblicato non deve comunque contenere l'intera valutazione, soprattutto qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza o divulgare informazioni riservate. In queste circostanze, la versione pubblicata può consistere soltanto in una sintesi delle principali risultanze del DPIA, nella conclusione del DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che il DPIA è stato condotto.

### **3. Attività conseguenti**

Quando il report DPIA è stato approvato, il Titolare procede con:

- pianificare eventuali interventi formativi per le persone coinvolte nel processo analizzato;
- verificare la presenza della policy privacy e informativa una volta che il trattamento sia reso accessibile agli utenti;
- monitorare l'organizzazione: ruoli e responsabilità, controlli interni, regole interne.

L'Amministrazione mantiene traccia delle DPIA effettuate attraverso il proprio Registro dei Trattamenti in formato elettronico.

La conservazione del Report DPIA è a cura del Responsabile della DPIA, quella del Registro dei Trattamenti è a cura dell'Ufficio Privacy, l'eventuale Consultazione preventiva all'Autorità di Controllo è a Protocollo.

Tali informazioni documentate devono essere conservate per il tempo congruo a dimostrare di aver svolto l'attività correttamente.

#### **4. Revisione DPIA**

Nel caso in cui il trattamento oggetto di valutazione d'impatto subisca dei cambiamenti che comportano modifiche sostanziali al trattamento dei dati, è necessario rivedere la DPIA effettuata in precedenza e modificarla in base ai cambiamenti effettuati.

È comunque buona regola procedere con una revisione annuale delle DPIA effettuate in modo da poter verificare che non siano necessari aggiornamenti e/o modifiche tenendo conto dello stato dell'arte.