PREDISPOSIZIONE DELLA DPIA PER GLI STUDI OSSERVAZIONALI RETROSPETTIVI

Redazione	Verifica	Approvazione
Referente di redazione: Cinzia Solazzo UFFICIO PRIVACY **Gruppo di redazione:** Elisa Tofani Francesco Maria Rossini Mascia Renzulli SOSD GARSP	Martina Frate UFFICIO PRIVACY Samantha Gomboso SOSD GARSP	Dott. Francesco Magris Direttore Dipartimento Amministrativo di Presidio *ad interim*
Firma	Firma	Firma

Parola chiave 1	Parola chiave 2	Parola chiave 3
Studi osservazionali retrospettivi	Predisposizione DPIA	

INDICE

1 Matrice delle versioni del documento 3
2 Scopo e campo di applicazione 3
3 Destinatari 3
4 DPIA: Data protection Impact Assessment 3
4.1 Fasi della DPIA 4
4.2 Criteri per la valutazione del rischio 4
4.3 DPIA: procedura operativa 5
4.4 Tempistiche 6
5 Ruoli e responsabilità 7
6 Terminologie e abbreviazioni 7
7 Bibliografia 7
8 Documenti interni collegati 7
9 Allegati 7

1 Matrice delle versioni del documento

Codifica	Versione	Data	Descrizione della modifica
DAP_PR_04	01	04/08/2025	Creazione del documento

2 Scopo e campo di applicazione

La presente procedura ha l'obiettivo di fornire linee guida sul flusso documentale/informativo tra le Unità Organizzative officiate per la predisposizione di una Valutazione d'Impatto sulla Protezione dei Dati (DPIA), relativamente agli studi osservazionali retrospettivi, in conformità al Regolamento (UE) 2016/679 (GDPR) e alle normative nazionali vigenti.

Il presente documento si applica a tutti gli studi osservazionali retrospettivi, condotti all'interno dell'Azienda Sanitaria Universitaria Friuli Centrale (ASUFC), nei quali vengono trattati dati personali e/o dati particolari (ad esempio, dati sanitari) raccolti originariamente per finalità di cura o precedentemente raccolti nell'ambito di altri studi clinici, per i quali non può non essere possibile raccogliere il Consenso Informato.

3 Destinatari

Il documento è rivolto a tutto il personale coinvolto nella progettazione, realizzazione, revisione e approvazione degli studi osservazionali retrospettivi, inclusi:

- Sperimentatore Principale e suoi collaboratori, responsabili della conduzione dello studio e della gestione dei dati raccolti;
- SOSD Gestione amministrativa ricerca, sperimentazioni e progetti finanziati, coinvolta nella supervisione di tale procedura;
- SOC Ufficio Privacy coinvolta nella predisposizione della DPIA;

Altre figure istituzionali preposte alla valutazione della conformità normativa, in base alle specifiche regolamentazioni aziendali e di settore.

4 DPIA: Data protection Impact Assessment

La Valutazione d'Impatto sulla Protezione dei Dati (DPIA) 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 prevede la raccolta e l'analisi di informazioni chiave, tra cui:

- Tipologia e natura dei dati trattati, con particolare attenzione ai dati sensibili o ad alto rischio (es. dati sanitari, genetici, biometrici);
- Finalità del trattamento, specificando gli obiettivi perseguiti e la necessità della raccolta dei dati;
- Base giuridica del trattamento, in conformità al GDPR e alle normative nazionali;
- Modalità di trattamento, inclusi i sistemi e le tecnologie utilizzate;
- Misure di sicurezza adottate, per garantire la protezione dei dati personali;
- Valutazione dei rischi e misure di mitigazione (contromisure), per ridurre l'impatto negativo del trattamento (in caso di rischio elevato).

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

4.1 Fasi della DPIA

La Valutazione d'Impatto sulla Protezione dei Dati (DPIA) è un processo strutturato per identificare e mitigare i rischi legati al trattamento dei dati personali, il tutto prima dell'approvazione finale. Le fasi principali includono:

1. **Identificazione del trattamento**
   - Descrizione dettagliata del trattamento dei dati, comprese finalità, basi giuridiche e categorie di dati trattati.
   - Identificazione degli attori coinvolti (titolare del trattamento, responsabile del trattamento, DPO, ecc.).
2. **Valutazione della necessità e proporzionalità**
   - Analisi dell'adeguatezza del trattamento rispetto agli obiettivi perseguiti.
   - Verifica del rispetto dei principi del GDPR (minimizzazione, trasparenza, liceità, limitazione della conservazione).
3. **Analisi dei rischi per i diritti e le libertà degli interessati**
   - Identificazione dei potenziali rischi derivanti dal trattamento dei dati.
   - Analisi del livello di rischio (basso, medio, alto) attraverso metodologie autorizzate (sistema Motore Unico Amministrativo).
4. **Definizione di eventuali contromisure**
   - Identificazione delle misure di sicurezza tecniche e organizzative per ridurre i rischi.
   - Valutazione dell'efficacia delle misure adottate.
5. **Consultazione con il DPO**
   - Il Responsabile della Protezione dei Dati (DPO) fornisce un parere sulla DPIA.
6. **Approvazione**
   - Approvazione della DPIA da parte del titolare del trattamento di ASUFC.
7. **Pubblicazione richiesta per i casi specifici previsti dall'Articolo 110 del Codice della Privacy**
   - Pubblicazione della DPIA all'interno del sito aziendale ASUFC, nella sezione dello studio cui fa riferimento.
   - Pubblicazione dell'informativa all'interno del sito aziendale ASUFC, nella sezione dello studio cui fa riferimento.

L'ufficio privacy si atterrà a dette indicazioni, mediante l'utilizzo di strumenti informatici messi a disposizione dall'Azienda.

4.2 Criteri per la valutazione del rischio

La valutazione del rischio nella DPIA si basa su un'analisi strutturata che determina l'impatto del trattamento sui diritti e le libertà degli interessati. Questa analisi è allineata ai principi e alle linee guida degli standard ISO 31000 (Risk Management – Principles and guidelines) e ISO 27001. I principali criteri di valutazione includono:

1. **Definizione del contesto**
   - Identificazione della natura, ambito di applicazione e finalità del trattamento.
2. **Tipologia di dati trattati**
   - Dati comuni (es. nome, cognome, contatti) → **basso rischio**
   - Dati particolari (es. sanitari, biometrici, genetici) → **alto rischio**
   - Dati relativi a condanne penali e reati → **rischio elevato**
3. **Identificazione del rischio**
   - Identificazione delle minacce (ossia degli eventi indesiderati che incidono su disponibilità, riservatezza e integrità dei dati personali oggetto di trattamento);
4. **Analisi del rischio**
   - Identificazione delle vulnerabilità che gravano sull'organizzazione;
   - Valutazione delle contromisure esistenti e della loro efficacia;

- Probabilità che un rischio si concretizzi (bassa, media, alta);
- Gravità dell'impatto sugli interessati (limitato, significativo, critico).

5. **Ponderazione del rischio**
   - Assegnazione di un livello di esposizione al rischio per ogni trattamento;
   - Applicazione di coefficienti di ponderazione per vulnerabilità e contromisure.
6. **Trattamento del rischio**
   - Predisposizione di un piano di mitigazione e gestione del rischio.
7. **Fattore di rischio**
   - L'algoritmo adottato per la valutazione del rischio è:

     $$R_T = f(V_T, P_T, D_T)$$

     dove:
     - RT è l'indice di rischio che insiste sul Trattamento, espresso in valori percentuali;
     - VT è l'indice di vulnerabilità degli asset coinvolti nel trattamento, tenuto conto delle contromisure, dirette o indirette, attuate e del livello di criticità espresso sul singolo asset;
     - PT è la probabilità di accadimento dell'evento indesiderato sul trattamento;
     - DT è la gravità delle conseguenze della concretizzazione dell'evento indesiderato sul trattamento.
   - I parametri di calcolo includono:
     - Peso vulnerabilità (PV): suscettibilità intrinseca degli asset;
     - Peso contromisure (PCM): misure dirette e indirette applicate;
     - Peso asset (PA): impatto degli asset sul trattamento;
     - Probabilità (P): frequenza storica di accadimento;
     - Danno (D): gravità delle conseguenze secondo le linee guida WP 248 Rev. 01.
8. **Indice di rischio**
   - Al termine della valutazione si otterrà l'indice di livello di rischio;
   - I possibili livelli di rischio sono:
     - Rischio molto basso;
     - Rischio basso;
     - Rischio medio;
     - Rischio alto;
     - Rischio molto alto.

La Valutazione fornisce indicazioni sulle azioni di contrasto e miglioramento da adottare.

4.3 DPIA: procedura operativa

Negli studi osservazionali retrospettivi, la DPIA è obbligatoria per garantire che il trattamento dei dati personali avvenga in conformità al GDPR e alle normative nazionali in ambito sanitario. La procedura operativa di ASUFC segue questi passaggi:

SPERIMENTATORE PRINCIPALE → SOSD GARSP

Lo Sperimentatore Principale inoltra alla SOSD GARSP i documenti sotto riportati, necessari all'Ufficio Privacy per la predisposizione della DPIA:

a) sinossi e protocollo dello studio;
b) questionario contenente le informazioni necessarie per la redazione della DPIA all'interno del quale è contenuta una parte relativa all'eventuale adesione all'art. 110 Codice Privacy (Allegato 1 - Istruttoria);

SOSD GARSP
Verifica la presenza e la completezza formale di tutti i documenti richiesti per la stesura della DPIA. La responsabilità dei contenuti di tali documenti è ad esclusivo carico dello Sperimentatore Principale.

SOSD GARSP → UFFICIO PRIVACY
La SOSD GARSP trasmette la documentazione dello Studio Clinico sottoposta alla valutazione del Comitato Etico competente e la documentazione necessaria per la predisposizione della DPIA all'Ufficio Privacy all'indirizzo mail: privacy@asufc.sanita.fvg.it.

UFFICIO PRIVACY
L'Ufficio Privacy svolge l'analisi di impatto del trattamento dei dati personali attraverso le seguenti attività:

- verifica della documentazione ricevuta;
- valutazione dei mezzi di trattamento utilizzati;
- identificazione del livello di rischio generale e specifico per il trattamento;
- analisi delle vulnerabilità e delle contromisure messe in atto;
- redazione dell'Informativa sul trattamento dei dati ex artt. 13 e 14 GDPR;
- trasmissione della documentazione al DPO per il parere finale.

In caso di necessità di chiarimenti e/o integrazioni, l'Ufficio Privacy si interfaccia direttamente con lo Sperimentatore Principale.

UFFICIO PRIVACY → SPERIMENTATORE PRINCIPALE
Una volta ottenuto il parere obbligatorio del DPO (Data Protection Officer), come previsto dal GDPR per assicurare la conformità e la gestione dei rischi, l'Ufficio Privacy trasmette la documentazione completa della DPIA allo Sperimentatore Principale e, per conoscenza, alla SOSD GARSP:

- cartella zippata contenente il livello di rischio generale e specifico per il trattamento, l'analisi delle vulnerabilità e delle contromisure messe in atto;
- parere del DPO;
- informativa ex art. 13 e 14 GDPR;
- estratto o documento di chiusura DPIA, a firma del Direttore Generale.

Oltre ai documenti sopra indicati costituenti la DPIA, viene inviato anche il registro per l'annotazione dei tentativi di contatto da utilizzare nel solo caso di applicazione dell'art. 110 Codice Privacy (Allegato 2 - Registro).

SOSD GARSP
A seguito dell'attivazione dello studio, la SOSD GARSP provvede alla sua pubblicazione, contestualmente all'informativa ex art. 13 e 14 GDPR e all'estratto della DPIA, sul sito istituzionale e dandone comunicazione ai diretti interessati e all'Ufficio Privacy tramite i canali ordinari.
L'onere di pubblicazione sussiste solo qualora si rientri nelle fattispecie disciplinate dall'art. 110 Codice Privacy.

UFFICIO PRIVACY
Se lo studio rientra nelle fattispecie disciplinate dall'art. 110 Codice Privacy, l'Ufficio Privacy inoltra la comunicazione al Garante.

4.4 Tempistiche

Il processo di valutazione e rilascio della DPIA richiede circa 60 giorni, salvo casi di particolare complessità che potrebbero estendere la tempistica.

5 Ruoli e responsabilità

Per ciascuna attività vengono indicate le responsabilità di ciascuna figura relativamente al suo specifico ambito di competenza.

Attività	Sperimentatore principale	SOSD GARSP	Uff. PRIVACY	DPO
Predisposizione della documentazione necessaria per la richiesta di DPIA	R			
Invio della documentazione alla SOSD GARSP	R	I		
Verifica della completezza formale dei documenti		R		
Trasmissione della documentazione all'Ufficio Privacy	I	R	I	
Redazione DPIA, informativa ex art. 14 GDPR ed estratto o chiusura DPIA	C		R	
Parere sulla DPIA			C	R
Invio documentazione finale allo Sperimentatore Principale e alla SOSD GARSP	I	I	R	
Comunicazione di pubblicazione studio	I	R	I	
Notifica al Garante (art. 110 Codice Privacy)	I	I	R	I

Legenda: R = Responsabilità generale sull'attività C = Collaborazione all'attività I = Informazione sull'attività

6 Terminologie e abbreviazioni

GARSP	Gestione Amministrativa Ricerca, Sperimentazioni e Progetti finanziati
SOSD	Struttura Operativa Semplice Dipartimentale
SOC	Struttura Operativa Complessa
GDPR	General Data Protection Regulation
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment

7 Bibliografia

Non prevista

8 Documenti interni collegati

DAP_RG_01: REGOLAMENTO SUL MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI "MOP" DELL'AZIENDA SANITARIA UNIVERSITARIA FRIULI CENTRALE

9 Allegati

Allegato 1 - Istruttoria
Allegato 2 - Registro