Parere del Responsabile della Protezione dei Dati (DPO)
DPIA – Biobanca IRCCS CRO Aviano

1. Premessa

Il presente parere è espresso dal Responsabile della Protezione dei Dati (Data Protection Officer – DPO) dell'IRCCS Centro di Riferimento Oncologico di Aviano ai sensi degli articoli 35, paragrafo 2, e 39, paragrafo 1, lettera c) del Regolamento (UE) 2016/679 (GDPR), con riferimento alla Data Protection Impact Assesment (DPIA) relativa ai trattamenti di dati personali connessi alle attività della Biobanca del CRO di Aviano.
Ai sensi dell'articolo 35 del GDPR, il Titolare del trattamento è tenuto a effettuare una valutazione d'impatto sulla protezione dei dati qualora un tipo di trattamento, in particolare se prevede l'uso di nuove tecnologie e tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Il DPO è stato coinvolto nel processo di valutazione ed ha esaminato la documentazione predisposta dal Titolare del trattamento e dalle strutture organizzative competenti, fornendo supporto e consulenza in relazione alla conformità del trattamento alla normativa in materia di protezione dei dati personali.
Il presente parere è formulato sulla base dell'analisi della DPIA e della documentazione disponibile alla data di redazione del presente documento.

2. Quadro normativo e regolatorio di riferimento

La valutazione è stata effettuata tenendo conto del quadro normativo europeo e nazionale applicabile ai trattamenti di dati personali in ambito sanitario e di ricerca scientifica, ed in particolare:

- ✓ Regolamento (UE) 2016/679 (GDPR), con particolare riferimento agli artt. 5, 9, 24, 25, 32, 35 e 89;
- ✓ Linee guida del Gruppo Articolo 29 (oggi EDPB) sulla DPIA – WP248 rev.01;
- ✓ Provvedimento del Garante per la protezione dei dati personali n. 467/2018 relativo all'elenco dei trattamenti soggetti a DPIA;
- ✓ Provvedimenti del Garante per la protezione dei dati personali n. 146/2019 e n. 298/2024;
- ✓ normativa e indirizzi nazionali in materia di ricerca scientifica e gestione di materiale biologico umano;
- ✓ standard tecnici e organizzativi richiamati nella DPIA, tra cui ISO 20387, ISO/IEC 27001 e linee guida BBMRI-ERIC.

Il contesto normativo di riferimento appare adeguatamente considerato nella DPIA esaminata.

3. Valutazione della descrizione del trattamento

Dall'esame della documentazione emerge che la DPIA contiene una descrizione sufficientemente dettagliata delle operazioni di trattamento connesse al funzionamento della Biobanca.
In particolare, risultano descritti:

- ✓ le finalità del trattamento, riconducibili alle attività istituzionali dell'IRCCS nell'ambito della ricerca biomedica e della diagnostica;
- ✓ le categorie di dati personali trattati, incluse categorie particolari di dati ai sensi dell'art. 9 GDPR, quali dati sanitari e dati genetici;
- ✓ le categorie di interessati, tra cui pazienti adulti, minori e soggetti deceduti;
- ✓ i flussi di trattamento relativi alla raccolta, registrazione, pseudonimizzazione, conservazione, utilizzo e cessione dei campioni biologici e dei dati associati;
- ✓ l'architettura organizzativa e tecnologica della Biobanca.

La descrizione del ciclo di vita dei campioni biologici e dei dati associati appare coerente con i requisiti previsti dall'art. 35 del GDPR.

4. Valutazione della liceità, necessità e proporzionalità del trattamento

Dalla DPIA risulta che i trattamenti effettuati dalla Biobanca si fondano su basi giuridiche conformi al GDPR.
In particolare:

- ✓ art. 9, par. 2, lett. a) GDPR – consenso esplicito dell'interessato;
- ✓ art. 9, par. 2, lett. j) GDPR – trattamento necessario per finalità di ricerca scientifica.

La DPIA evidenzia inoltre il rispetto dei principi di cui all'articolo 5 del GDPR, tra cui limitazione delle finalità, minimizzazione dei dati, limitazione della conservazione e integrità e riservatezza.
L'utilizzo sistematico di tecniche di pseudonimizzazione e il controllo degli accessi basato sui ruoli contribuiscono a garantire la proporzionalità del trattamento rispetto alle finalità perseguite.

5. Valutazione delle misure tecniche e organizzative

La DPIA descrive un insieme articolato di misure tecniche, organizzative e fisiche finalizzate a garantire un adeguato livello di sicurezza dei dati personali ai sensi dell'art. 32 del GDPR.
Tra le principali misure adottate si evidenziano:

- ✓ pseudonimizzazione dei dati e dei campioni biologici;
- ✓ cifratura dei dati in transito e a riposo;
- ✓ controllo degli accessi logici;
- ✓ sistemi di logging e audit trail;
- ✓ sistemi di monitoraggio degli eventi di sicurezza (SIEM);
- ✓ procedure di backup e disaster recovery;
- ✓ procedure organizzative formalizzate (SOP);
- ✓ misure fisiche di protezione dei locali e delle infrastrutture.

Le misure individuate risultano coerenti con la natura dei dati trattati e con i rischi identificati nella DPIA.

6. Valutazione dei rischi

La DPIA adotta una metodologia di analisi del rischio basata su una matrice impatto × probabilità.
Tra i principali scenari di rischio analizzati figurano:

- ✓ accessi non autorizzati ai dati o ai campioni biologici;
- ✓ perdita o alterazione dei dati;
- ✓ errori di associazione tra campioni biologici e dati clinici;
- ✓ indisponibilità dei sistemi informativi o delle infrastrutture di conservazione;
- ✓ rischio di re-identificazione degli interessati.

Le misure di mitigazione previste consentono di ridurre il rischio iniziale ad un livello residuo complessivamente classificato come medio-basso.

7. Raccomandazioni

Nel quadro di un approccio di miglioramento continuo della sicurezza e della protezione dei dati personali, il DPO formula alcune raccomandazioni:

- ✓ rafforzare l'utilizzo di autenticazione multifattore (MFA) per gli accessi ai sistemi critici;
- ✓ mantenere aggiornati i modelli contrattuali utilizzati per la cessione di campioni e dati (MTA/DTA);

- ✓ documentare periodicamente i test di disaster recovery e business continuity;
- ✓ proseguire con attività di audit e monitoraggio delle misure di sicurezza.

8. Conclusioni

Alla luce delle verifiche effettuate e della documentazione esaminata, il Responsabile della Protezione dei Dati ritiene che:

- ✓ la DPIA sia stata redatta in conformità ai requisiti previsti dall'articolo 35 del GDPR;
- ✓ i trattamenti di dati personali connessi alle attività della Biobanca risultino coerenti con il quadro normativo vigente;
- ✓ le misure tecniche e organizzative individuate risultino adeguate rispetto ai rischi identificati;
- ✓ il rischio residuo per i diritti e le libertà degli interessati possa essere considerato accettabile.

Pertanto, il DPO esprime parere favorevole alla prosecuzione delle attività di trattamento, fermo restando il monitoraggio periodico delle misure di sicurezza adottate.

Padova, 28/03/2026

Il Responsabile della Protezione dei Dati
Avv. Luigi Rufo

Luigi Rufo
28.03.2026
13:26:14
GMT+01:00