MultiMedica Spa

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

Studio Retinal (Effetto delle infezioni da SARS-Cov-2- sulla struttura retinica nei pazienti con diabete mellito)
Anno 2024

Il documento è basato sulle linee guida rilasciate dalle Autorità di controllo europee, sulla ISO/IEC 29134 e sui più comuni standard di riferimento in materia, i quali forniscono elementi utili per l'identificazione, l'analisi e la valutazione del rischio di un trattamento. Nella valutazione del rischio non si tiene conto soltanto della sicurezza del trattamento in sé ma anche agli effetti complessivi di quest'ultimo sui diritti e le libertà degli interessati.

Art. 35 Regolamento (UE) 27 aprile 2016 n. 679

1.Quando un tipo di 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, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2.Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3.La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a)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; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4.L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5.L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6.Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7.La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8.Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto

da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9.Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10.Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11.Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Titolare del trattamento

Ragione sociale	**MultiMedica Spa**
Sede legale	Milano, Via Fantoli 16/15
Sede operativa 1	IRCCS MultiMedica - Sesto S.G., Via Milanese 300
Telefono	02/2420.9288
E-mail	privacy@multimedica.it
PEC	direzione.multimedica@promopec.it

Data Protection Officer (DPO)

Nome	Marco Maglio
Contatto	rpd@multimedica.it

Descrizione del trattamento

Descrizione del trattamento	Studio Retinal (Effetto delle infezioni da SARS-Cov-2- sulla struttura retinica nei pazienti con diabete mellito)

CONTESTO

Panoramica
Quali sono le responsabilità legate al trattamento?
Con questo studio l'IRCCS MultiMedica in qualità di soggetto promotore, nell'ambito delle specifiche attività istituzionali di ricerca, intende perseguire gli obiettivi previsti dal protocollo di ricerca autorizzato dal Comitato Etico IRCCS MultiMedica sezione del Comitato Etico IRCCS Lombardia.
Si è in possesso di certificazioni o codici di condotta legati alla protezione dei dati personali?
L' IRCCS MultiMedica è in possesso dei requisiti ministeriali previsti per l'accreditamento e l'erogazione di attività di cura e ricerca. L'associazione imprenditoriale a cui la Società aderisce non ha adottato un codice di condotta. Si precisa che l'attività di ricerca viene condotta ai sensi della normativa nazionale ed internazionale, convenzioni, direttive e regolamenti vigenti.
Qual è il trattamento in considerazione?
Trattamento di dati personali e particolari per il raggiungimento degli obiettivi prefissati dal protocollo. Il trattamento prevede la raccolta, l'analisi (raffronto, elaborazione), archiviazione dei dati personali e particolari dei soggetti reclutati. Il Trattamento riguarda i dati personali di pazienti raccolti nell'ambito di visite oculistiche: nel dettaglio, vengono trattati dati personali comuni (nome, cognome, sesso, età, data di nascita) e dati personali particolari (es. fotografia fondo retinico, dati vascolari retina, BMI ed altri dati sanitari connessi alla patologia/cura, dati risultanti dalle analisi sul campione ematico, dato su pregresso covid), per successive analisi finalizzate al raggiungimento degli obiettivi della ricerca. Le categorie di dati vengono trattati secondo le disposizioni in materia di corretto trattamento dei dati ed a titolo esemplificativo in conformità ai principi di minimizzazione, pseudonomizzazione, pertinenza, limitazione, sicurezza e limite temporale alla conservazione. La scelta dei pazienti arruolati per lo studio implica la classificazione dei soggetti, secondo criteri di inclusione/esclusione.

Dati, processi e risorse di supporto	
Dati personali trattati	Codice fiscale, Dati anagrafici, Data di nascita, Codice univoco, Dati personali
Dati particolari trattati	Dati particolari, Dati biometrici - retina, Dati particolari - Dati inerenti lo stato di salute, BMI - indice di massa corporea, Pregressa patologia covid , vaccinazioni covid, campione biologico
Dati giudiziari trattati	N.T.
Categorie di soggetti interessati	Soggetti arruolati , Pazienti
Qual è il ciclo di vita dei dati?	I dati personali e particolari del paziente vengono raccolti nel corso di visite di controllo oculistiche eseguite nell'ambito della normale pratica clinica. Qualora il medico ravvisi nel paziente l'idoneità di quest'ultimo all'inclusione nello studio clinico gli propone la partecipazione allo studio. Al paziente viene chiesto di sottoscrivere consenso informato alla partecipazione allo studio e al trattamento dei dati nell'ambito della sperimentazione. I dati raccolti per la finalità di ricerca vengono estratti e strutturati in un data base che verrà utilizzato per le analisi eseguite. I dati presenti nel data base sono pseudonimizzati. Alla conclusione dello studio i dati sono archiviati secondo quanto previsto dalla normativa in materia.
Asset coinvolti	File Excel, EPR Replay , e-visit, Archivio cartaceo corrente, Personal comuputer, ADT Appheal

PRINCIPI FONDAMENTALI

Proporzionalità, necessità	
Finalità	Ricerca scientifica
Gli scopi del trattamento sono specifici, espliciti e legittimi? (Principio di limitazione della finalità)	Si ritiene che il trattamento sia necessario in quanto la ricerca scientifica è un elemento strategico fondamentale per raggiungere e mantenere livelli di eccellenza nell'ambito dell'attività scientifica di interesse pubblico, conformemente alle pertinenti norme etiche e metodologiche settoriali e in conformità delle buone prassi [Fonte: Considerando 159 GDPR] e per garantire ai cittadini una sanità efficiente e rispondente ai reali bisogni di assistenza e cura del Paese, allo scopo di far avanzare in modo significativo le conoscenze su aspetti importanti delle diverse condizioni patologiche e/o di promuovere lo sviluppo di opzioni (di diagnosi, trattamento, ecc.) innovative (theory enhancing), nonché fornire soluzioni a problemi specifici e concreti e produrre informazioni utili a indirizzare positivamente le scelte dei diversi decisori (change promoting) [Fonte: Ministero della Salute Direzione generale della ricerca e della innovazione in sanità, Programma Nazionale della Ricerca Sanitaria PNRS 2020-2022, p. 4]. Si ritiene che i dati trattati siano considerati proporzionati rispetto ai fini per i quali vengono trattati in quanto vengono utilizzati per i soli fini di ricerca scientifica i dati necessari raccolti nell'ambito di visite e prestazioni oculistiche e analisi di laboratorio di ricerca: nel dettaglio, vengono trattati dati personali comuni (nome, cognome, sesso, età, data di nascita) e dati personali particolari (fondo retinico, dati vascolari retina, indice di massa corporea ed altri dati sanitari connessi alla patologia/cura, dati risultanti dalle analisi sul campione ematico, dato su pregresso covid), per successive analisi finalizzate al raggiungimento degli obiettivi della ricerca. Le finalità del trattamento sono legittime, specifiche ed esplicitate al paziente nel corso della fase di inclusione nello studio. Ai pazienti che intendono partecipare allo studio viene richiesto il rilascio del consenso informato che dettaglia, nello specifico, la tipologia di dati raccolti e le finalità per i quali gli stessi saranno trattati. Il consenso informato condiviso con i pazienti prevede l'esercizio dei diritti da parte degli stessi secondo specifiche modalità e canali. Il consenso informato regolamenta l'esercizio dei diritti degli interessati e definisce puntualmente i canali di esercizio degli stessi.
Quali sono le basi giuridiche che rendono il trattamento legittimo?	Consenso dell'interessato
I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati? (Principio di minimizzazione dei dati)	I trattamento dei dati personali avviene per le sole finalità dichiarate nell'informativa, ovvero l'analisi dei dati personali richiede anche l'elaborazione sulla base di metodi statistici; analisi per la verifica della correlazione tra condizioni patologiche specifiche, per fini di prevenzione, diagnosi e/o miglioramento del trattamento/cura; disseminare (diffondere) i risultati della ricerca in favore della comunità scientifica e permettere la verifica dei risultati, anche attraverso la pubblicazione dei dati aggregati e non aggregati, comunque sempre anonimizzati, tramite appositi canali (es. riviste scientifiche, repository pubblici); ed esecuzione di attività di ricerca scientifica sulla base degli obiettivi degli studi. Si ritiene che il trattamento sia necessario in quanto la ricerca scientifica è un elemento strategico fondamentale per raggiungere e mantenere livelli di eccellenza nell'ambito dell'attività scientifica di interesse pubblico, conformemente alle pertinenze norme etiche e metodologiche settoriali e in conformità delle buone prassi [Fonti: Considerando 159 GDPR e Ministero Salute]. Si ritiene inoltre che i dati trattati siano considerati proporzionati rispetto ai fini per i quali vengono trattati in

	quanto vengono utilizzati ai fini di ricerca scientifica esclusivamente i dati necessari raccolti nell'ambito di visite oculistiche: nel dettaglio, vengono trattati dati personali comuni (nome, cognome, sesso, età, data di nascita) e dati personali particolari (fotografia fondo retinico, dati vascolari retina, BMI - indice di massa corporea - ed altri dati sanitari connessi alla patologia/cura, dati risultanti dalle analisi sul campione ematico, dato su pregresso covid), per successive analisi finalizzate al raggiungimento degli obiettivi della ricerca.
I dati sono esatti e, se necessario, aggiornati? (Principio di esattezza)	Si, dati sono esatti. Al momento dell' accettazione, quindi previa proposta di inclusione dello studio, l'operatore che si occupa della parte amministrativa verifica sempre l'indentità del soggetto. Una volta che il paziente viene reclutato nello studio avviene una separazione dei dati raccolti per finalità di assistenza sanitaria ed erogazioni di prestazioni dai dati clinici che saranno necessari per lo studio. I dati sono raccolti dai pazienti stessi nell'ambito di visite oculistiche e non vengono alterati né modificati. In caso di revoca del consenso i dati non vengono più utilizzati.
Qual è la durata della conservazione dei dati?	I dati verranno conservati con tecniche e metodologie sicure. Il periodo di conservazione corrisponde alla durata dello Studio e, in ogni caso, non è superiore al termine disposto dal Provvedimento dell'Autorità in tema di ricerca scientifica come riportato all'interno del Registro dei Trattamenti.
I dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato? (Principio di liceità, correttezza e trasparenza)	Si, i dati sono trattati in modo lecito , corretto e trasparente e previa rilascio da parte dell'interessato di inidoneo consenso. Soltanto soggetti preposti e adeguatamente istruiti ai sensi dell' art 29 GDPR avranno accesso ai dati.

Controlli per proteggere i diritti personali dei soggetti interessati	
I soggetti interessati sono informati del trattamento?	Si, tramite sottoscrizione e rilascio di consenso tramite idonea informativa.
Se la base giuridica è il consenso, descrivere come si ottiene il consenso dei soggetti interessati?	Ai pazienti che intendono partecipare allo studio viene richiesto il rilascio del consenso informato che dettaglia, nello specifico, la tipologia di dati raccolti e le finalità per i quali gli stessi saranno trattati.
I soggetti interessati come esercitano i loro diritti di accesso alla portabilità dei dati?	Il consenso informato regolamenta l'esercizio dei diritti degli interessati e definisce puntualmente i canali di esercizio degli stessi.
I soggetti interessati come esercitano i loro diritti alla rettifica e alla cancellazione dei dati?	I soggetto interessati esercitano i diritti nelle forme e con le modalità di legge e comunque richiamate nell'informativa.
I soggetti interessati come esercitano i loro diritti all'opposizione al trattamento dei dati?	I soggetto interessati esercitano i diritti nelle forme e con le modalità di legge e comunque richiamate nell'informativa.
Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un atto giuridico?	Si, l' Azienda in occasione della stipula di ciascun nuovo ordine o contratto chiede la compilazione e sottoscrizione di un atto di nomina ai sensi dell' art 28 GDPR. Contestualmente viene richiesta la compilazione di una check list volta a mappare e valutare le misure tecniche, organizzative e di sicurezza adottate dal fornitore del servizio. Gli atti di nomina vengono periodicamente rivisti ed aggiornati.
Nel caso di trasferimento di dati extra UE, che garanzie adeguate sono presenti?	N.P.

RISCHI

Accesso illegittimo ai dati personali		
Descrizione dell'impatto sugli interessati se il rischio dovesse concretizzarsi	Un eventuale accesso illegittimo ai dati esporrebbe al rischio di accesso illegittimo ad dati del paziente incluso nello studio.	
Minacce	Spionaggio degli individui, Carenza di consapevolezza, disattenzione o incuria, Lettura non autorizzata di dati da schermate video, Abuso di privilegi da parte di utenti con profilo autorizzativo ampio, Accesso e lettura non autorizzata di dati su archivi informatici, Accesso non autorizzato ai servizi di rete e agli applicativi, Utilizzo non corretto di dispositivi o strumenti informatici	
Rischi	Risorsa umana interna che genera il rischio deliberatamente, Risorsa umana esterna che genera il rischio deliberatamente	
Quali dei controlli identificati contribuiscono a gestire il rischio?	Chiavi di accesso ai locali, Illuminazione di emergenza, Riservatezza della postazione, Data retention policy, Registro dei trattamenti, RPD/DPO, Formazione periodica del personale, Controllo accessi fisici, Procedura di autenticazione, Esistenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento, Policy pulizia desktop	
Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?	2	I soggetti interessati potranno incontrare inconvenienti significativi che saranno in grado di superare malgrado non poche difficoltà (es. costi aggiuntivi, diniego d'accesso ai business service, stress, paura, ecc).
Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati?	2	Il suo verificarsi richiederebbe circostanze non comuni e di poca probabilità;Si sono verificati pochi fatti analoghi;Il suo verificarsi susciterebbe modesta sorpresa

Modifiche indesiderate dei dati personali		
Descrizione dell'impatto sugli interessati se il rischio dovesse concretizzarsi	L'eventuale modifica di dati personali di soggetti arruolati nello studio potrebbe comportare l'alterazione dei risultati delle analisi necessarie per la realizzazione dello studio.	
Minacce	Furto credenziali di autenticazione, Carenza di consapevolezza, disattenzione o incuria, Lettura non autorizzata di dati da schermate video, Minaccia fisica di origine umana intenzionale volta a compromettere integrità fisica degli apparati e infrastrutture, Accessi non autorizzati a locali/reparti ad accesso ristretto, Utilizzo non corretto di dispositivi o strumenti informatici , Manipolazione di individui	
Rischi	Risorsa umana interna che genera il rischio accidentalmente, Risorsa umana esterna che genera il rischio deliberatamente	
Quali dei controlli identificati contribuiscono a gestire il rischio?	Conservazione dei log, Backup, Autenticazione informatica, Formazione periodica del personale	
Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?	1	Gli interessati non saranno coinvolti e/o incontreranno inconvenienti superabili senza difficoltà
Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati?	1	Il suo verificarsi richiederebbe la concomitanza di più eventi poco probabili;Non si sono mai verificati fatti analoghi;Il suo verificarsi susciterebbe incredulità

Scomparsa di dati personali		
Descrizione dell'impatto sugli interessati se il rischio dovesse concretizzarsi	La scomparsa dei dati potrebbe non consentire il raggiungimento degli obiettivi fissati dallo studio.	
Minacce	Furto o smarrimento di dati, Danneggiamento/distruzione di documenti cartacei, condizioni lavorative non adeguate, Errori umani accidentali	
Rischi	Risorsa umana interna che genera il rischio accidentalmente, Risorsa umana esterna che genera il rischio deliberatamente	
Quali dei controlli identificati contribuiscono a gestire il rischio?	Firewall, Backup, Archivio chiuso a chiave, Formazione periodica del personale, Conservazione dei log	
Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?	1	Gli interessati non saranno coinvolti e/o incontreranno inconvenienti superabili senza difficoltà
Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati?	1	Il suo verificarsi richiederebbe la concomitanza di più eventi poco probabili;Non si sono mai verificati fatti analoghi;Il suo verificarsi susciterebbe incredulità

MAPPATURA DEL RISCHIO

Mappa di calore

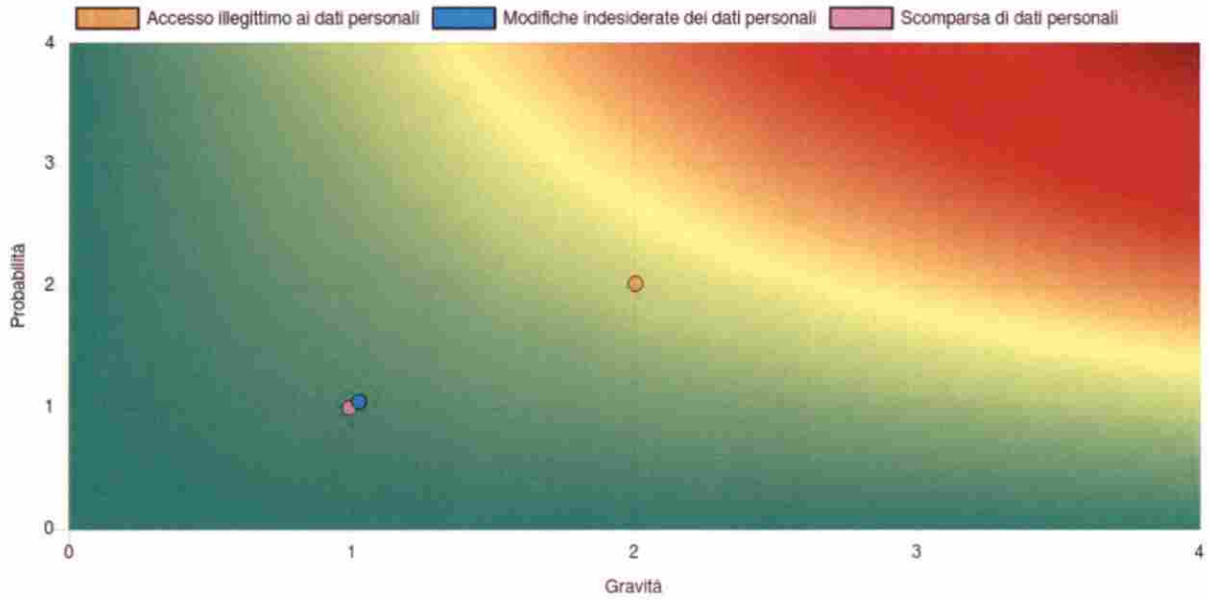
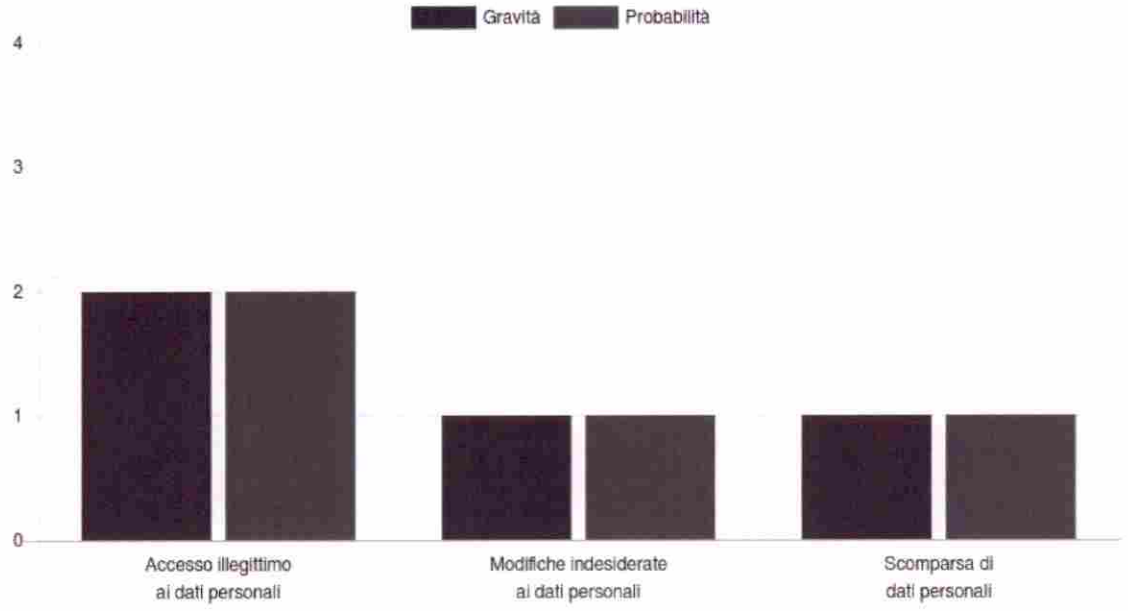
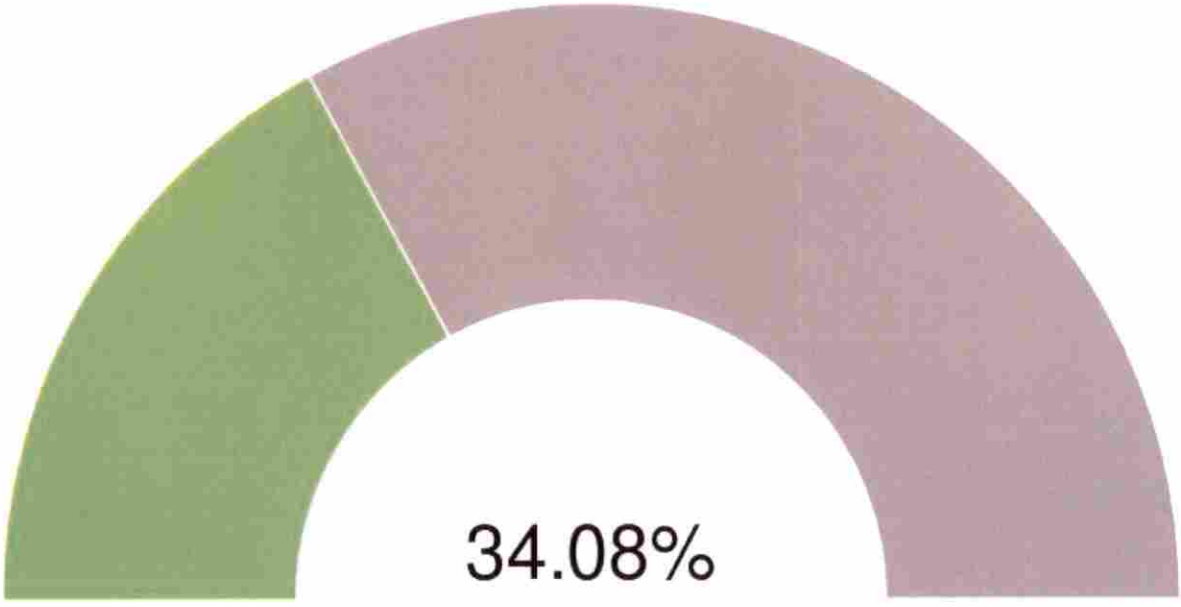


Grafico radar

Istogramma



Rischio totale



CONVALIDA

Convalida	
Parere DPO	Il trattamento di dati personali oggetto della presente valutazione di impatto risulta strutturato nel rispetto dei criteri di privacy by design e privacy by default previsti dall'art. 25 del Regolamento UE 2016/679 e dei principi previsti dall'art. 5 del medesimo Regolamento. Le misure di sicurezza adottate sono adeguate e tengono conto dei ruoli del trattamento e della natura dei dati personali trattati. Questo porta a ritenere che il trattamento può essere effettuato e non comporta rischi elevati per i diritti e le libertà fondamentali degli interessati.
Parere soggetti interessati	Non previsto

Piano d'azione	
Piano d'azione	Il Titolare del trattamento monitora la situazione attuale nonché lo stato di attuazione delle misure volte a mitigare i rischi emersi dallo svolgimento della DPIA.

Rev.	Data revisione	Modifiche
1	10/01/2024	REV.1

Il Titolare del trattamento

Multimedica Spa