

DPIA

PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) Missione 4 “Istruzione e Ricerca” - Componente C2 Investimento 1.1, “Fondo per il Programma Nazionale di Ricerca e Progetti di Rilevante Interesse Nazionale (PRIN)” Decreto Direttoriale n. 1409 del 14 settembre 2022, Avviso pubblico per la presentazione di Progetti di ricerca di Rilevante Interesse Nazionale (PRIN) da finanziare nell’ambito del PNRR

Progetto n° P2022JSLZW: “Assessing conflict of interests – ACOI” 30.04.2024

Premessa

Utilizzando una valutazione qualitativa del rischio, svolta sulla base di indicazioni fornite nel documento “Manuale RPD” delle Autorità garanti, elaborato per il programma “T4Data” e riportate nello schema in allegato 1 di questa DPIA, si ritiene che l’impatto derivante sugli interessati dalla violazione della riservatezza dei dati sia Alto, potendo generare pregiudizi, schedature, ricatti e altre ricadute che possono essere superate con difficoltà sulla vita sociale e personale degli interessati.

Pertanto, pur ritenendo bassa la probabilità del verificarsi di minacce (come da calcolo effettuato sulla tabella riportata in allegato 2 alla DPIA) si è proceduto a svolgere la DPIA essendo medio-alta la valutazione del rischio complessivo.

Panoramica del trattamento per quanto di rilievo nei trattamenti di dati personali

Il progetto di ricerca PRIN PNRR 2022 - “Assessing Conflict of Interest- ACOI”, intende sperimentare e studiare le potenzialità di un sistema di mappatura, evidenziazione e analisi delle partecipazioni, dei legami familiari e degli interessi economici di persone fisiche con incarichi pubblici che sono soggetti alla dichiarazione di assenza di conflitto di interessi; l’attività di ricerca intende studiare vantaggi, limiti, e opportunità che la mappatura degli interessi può offrire nelle attività di controllo circa l’insussistenza di situazioni di conflitto d’interessi. Il trattamento dei dati personali consiste nel mappare gli interessi professionali e economico-finanziari degli interessati, fornendo una visualizzazione dei rapporti in cui si esprimono questi interessi. La mappatura, che produce una visualizzazione dei rapporti che fanno capo all’interessato, è poi posta a confronto con gli interessi pubblici (primari e secondari) che il soggetto è tenuto a perseguire/curare, nell’esercizio delle sue funzioni. La sperimentazione intende testare diverse soluzioni di “normalizzazione” degli interessi pubblici, così da consentire un’analisi semi-automatizzata, volta alla evidenziazione di situazioni in cui uno o più tra gli interessi mappati e quelli pubblici possono risultare, potenzialmente, in conflitto (red flag). Lo studio e la sperimentazione di questa soluzione di analisi mira a fornire indicazioni sui vantaggi di questo approccio, sulla capacità di individuare, selezionare ed evidenziare correttamente le situazioni potenziali di conflitto, sui problemi relativi alle informazioni necessarie per la sua esecuzione, e sulle carenze informative esistenti. In prospettiva (ma ciò non è oggetto del progetto di ricerca ACOI), qualora la soluzione sperimentata fornisse indicazioni positive in termini di concreta fattibilità, potrebbe fornire la base per lo sviluppo di una soluzione da applicare a supporto (in funzione istruttoria) delle attività di controllo circa la veridicità delle dichiarazioni.

La mappatura avviene mediante l’interrogazione, l’analisi e la combinazione di banche dati diversificate (interessi e partecipazioni societarie, rapporti familiari, informazioni catastali), anche mediante il connettore rappresentato dal codice fiscale. Il sistema intende testare il meccanismo di analisi anche mediante il ricorso a dati da ritrarsi dalle banche dati contenenti informazioni anagrafiche (via ANPR, in titolarità al Ministero dell’Interno), al fine di evidenziare anche le mappe degli interessi che facciano capo ai congiunti rilevanti ai fini del conflitto d’interessi.

Ambito e natura del trattamento: il trattamento avviene nell'ambito di una attività di ricerca scientifica, su un progetto di interesse pubblico (PRIN) finanziato su fondi PNRR. La natura del trattamento è di carattere sperimentale, finalizzato a verificare come determinate tecniche di combinazione ed integrazione di dati personali può fornire risorse conoscitive utili all'esercizio delle funzioni di prevenzione della corruzione amministrativa.

Contesto: il contesto di riferimento è rappresentato dalle attività di prevenzione della corruzione amministrativa che le amministrazioni sono tenute a svolgere in modo rutinario, al fine di preservare l'imparzialità dell'agire pubblico e la fiducia del pubblico. In tale contesto, le attività di verifica del conflitto d'interessi costituiscono uno snodo essenziale, dal momento che il conflitto d'interessi costituisce l'istituto cardine della prevenzione della corruzione. In tale contesto, tuttavia, l'amministrazione (chiamata ad acquisire le dichiarazioni di assenza di conflitto d'interessi, e a verificarne la veridicità) si trova a soffrire di una strutturale condizione di asimmetria informativa. Infatti, generalmente è il soggetto direttamente interessato dalla situazione di conflitto di interessi a doverne darne informazione all'amministrazione (tramite un modulo di autodichiarazione). Se tale modalità di gestione dell'istituto risponde ad un canone di appropriatezza, dal momento che – nella generalità dei casi – è il soggetto interessato ad avere (migliore, piena, e precisa) conoscenza della situazione in questione, allo stesso tempo questo meccanismo di emersione del conflitto d'interessi rivela anche la strutturale condizione di asimmetria informativa in cui si trova ad operare l'amministrazione, costretta (per le citate ragioni di appropriatezza conoscitiva) a ricorrere alle dichiarazioni dei soggetti interessati per avere contezza delle situazioni di conflitto d'interessi, così da potervi porre rimedio secondo quanto indicato dalla disciplina normativa.

Finalità: il progetto di ricerca PRIN PNRR 2022 "ACOI" ha come finalità quella di sperimentare una possibile soluzione utile a ridurre la asimmetrie informative dell'amministrazione, nella gestione dei compiti di verifica delle dichiarazioni sull'assenza del conflitto d'interessi. Il progetto di ricerca mira a studiare, analizzare e verificare una tecnica di ricostruzione e mappatura semi-automatizzata, volta a mappare gli interessi personali, patrimoniali ed economici dei soggetti che esercitano funzioni pubbliche e che sono tenuti a dichiarare l'assenza di conflitto d'interessi. Così facendo, la ricerca intende a studiare la fattibilità, i vantaggi e le problematiche di un meccanismo di analisi della mappa di interessi che fanno capo al dichiarante, mappa che consenta di rilevare in modo sistematico profili di potenziali situazioni di conflitto d'interessi (evidenziazione di *red flag*).

Dati personali trattati

➤ Tipologia di dati

Per ciascun interessato saranno raccolti i seguenti dati dalle fonti con essi citate:

- Dati anagrafici e dichiarazione di insussistenza conflitto di interesse: sezione Amministrazione trasparente dei siti istituzionali di PA;
- Dati anagrafici: nome e cognome; sesso; data e luogo di nascita; codice fiscale; dati attinenti a legami familiari (fonte Anagrafe Nazionale Popolazione residente)
- Dati patrimoniali e societari: informazioni su partecipazioni azionarie o ruoli apicali in imprese registrate, quali soci/titolari, amministratori, direttori, sindaci, di soggetti persone fisiche (fonte: Bureau van Dijk Orbis);
- Dati catastali: informazioni su proprietà immobiliari intestate a determinati soggetti e su co-intestazioni (fonte: Cerved);
- Raccolta di informazioni sullo svolgimento di incarichi pubblici (sezione Amministrazione trasparente dei siti istituzionali di PA)

I dati personali utilizzati sono **dati comuni**, già pubblicati nei siti dell'Amministrazione trasparente. Va sottolineato che la pubblicazione in amministrazione trasparente risponde in modo specifico ed esplicito ad

abilitare l'esercizio di attività di controllo pubblico e diffuso (art. 1 del d.lgs. 33/2013), con particolare riferimento alla prevenzione della corruzione amministrativa. La verifica e la gestione dei conflitti d'interesse (e quindi, anche l'attività di ricerca scientifica funzionale), anche sulla base di dati resi disponibili sulle sezioni Amministrazione trasparente, costituisce uno dei principali istituti di prevenzione della corruzione amministrativa.

Il prototipo è impostato fin dall'origine per integrare anche i dati e le informazioni relative ai legami familiari, da ricavare mediante interrogazione della banca dati nazionale ANPR (Anagrafe Nazionale delle Persone Residenti). Attualmente l'accesso all'ANPR non è ancora stato acquisito, ma sono in corso contatti con l'amministrazione dell'Interno.

Per la individuazione dei legami familiari, è stato chiesto al Ministero degli Interni di poter disporre dei dati anagrafici minimali delle persone aventi un legame di parentela con i soggetti che integrano il campione, selezionato come esposto. Il Ministero ritiene legittima la richiesta, ed è intenzionato ad accoglierla, in base ai seguenti presupposti:

- L'Università degli Studi di Perugia ha in essere l'esecuzione di un'attività di ricerca di rilevante interesse pubblico, come attestato dall'ottenimento del finanziamento di un progetto di ricerca di rilevante interesse nazionale (PRIN). L'attività di trattamento poggia pertanto sulla base giuridica di cui all'art. 6 par.1 lett. e) del Regolamento UE 2016/679 GDPR (vedi più nel dettaglio, **qui**: <https://acoi.scipol.unipg.it/basi-di-liceita-del-trattamento/>)
- Secondo le previsioni di cui all'art. 2-ter del D.Lgs. 196/2003 vigente, la comunicazione tra titolari che effettuano trattamenti di dati personali (non ricompresi nelle categorie di dati particolari di cui all'art. 9 par. 1 GDPR né relativi a condanne penali e reati di cui all'art. 10 GDPR), è consentita nei casi previsti dai commi 1 e 1-bis del medesimo articolo.
- La ricostruzione dei legami familiari è indispensabile alla mappatura degli interessi che fanno capo ai dichiaranti, dal momento che la nozione di conflitto di interessi copre gli interessi propri del soggetto che esercita la funzione e quelli dei suoi parenti o affini entro il secondo grado. Lo studio, pertanto, non può essere condotto senza completare l'analisi con la ricostruzione della mappa degli interessi che fanno capo ai familiari dei soggetti che sono presi come campione di sperimentazione.
- Al fine di assicurare una qualità elevata delle correlazioni familiari, soprattutto in relazione ai soggetti conviventi con il dichiarante, la banca dati ANPR risulta quella maggiormente qualificata, nonché l'unica fonte in grado di fornire in modo sistematico e aggiornato tali informazioni.
- Pertanto, è stata attivata la richiesta al Ministero degli Interni, titolare di tale banca dati nel perseguimento di finalità di interesse pubblico, di comunicare il set di informazioni minime necessarie correlate ai dati del dichiarante. Tale comunicazione (ed il trattamento dei dati così acquisiti al progetto) è legittimata dalle previsioni di cui all' art. 2-ter del d.lgs 196/2003 vigente (su cui, più nel dettaglio, vedi, le **"Basi legali che rendono lecito il trattamento"**, **qui**: <https://acoi.scipol.unipg.it/basi-di-liceita-del-trattamento/>)

➤ **Categorie di interessati:**

- Soggetti titolari di una dichiarazione di assenza di conflitto d'interesse accessibile nella sezione Amministrazione trasparente delle seguenti PA:
- Soggetti aventi legame di parentela fino al secondo grado con la categoria di interessati al punto precedente; coniuge; conviventi..

➤ **Numerosità dei soggetti interessati.** La mole dei dati personali coinvolti nel trattamento (e quindi dei soggetti interessati) è di circa 600 interessati in quanto soggetti esercitanti funzioni pubbliche, cui si aggiungono una stima potenziale di circa altre 2000 interessati (soggetti legati da legame di parentela

con i soggetti esercitanti funzioni pubbliche), per un totale di circa 2600 interessati dal trattamento. I dati dei 600 interessati sono stati tratti dai siti del Comune di Milano, del Comune di Perugia, Regione Lombardia e Regione Umbria; Ministero dell'Interno, Ministero della Salute, Ministero del Made in Italy, tramite interrogazione della sezione amministrazione trasparenza, sezione incarichi dirigenziali.

➤ **Ambito geografico:** Italia

➤ **Durata del trattamento:**

- I dati di tipo A (vedi *infra*) saranno trattati per il tempo strettamente necessario all'applicazione della funzione di **hash unidirezionale**, a fini di pseudonimizzazione, sotto l'esclusivo controllo del titolare del trattamento. Una volta avvenuta l'operazione di pseudonimizzazione, e svolte le opportune verifiche circa la qualità e la rispondenza alle esigenze della ricerca dei dati pseudonimizzati così ottenuti, i dati personali di origine saranno cancellati.
- I dati di tipo B (vedi *infra*) saranno trattati per quanto opportuno e necessario alle finalità del progetto di ricerca, anche con riferimento alle fasi ulteriori (oltre il termine di conclusione delle attività ufficiali), quali ad esempio la diffusione e la discussione dei risultati del progetto di ricerca. In ogni caso, la diffusione e la discussione dei dati avverrà con modalità tali da garantire l'anonimato degli interessati dal trattamento.

➤ **Durata della conservazione:**

- I dati di tipo A (vedi *infra*, **Granularità del trattamento**) saranno conservati per il tempo necessario alle attività di pseudonimizzazione (tramite applicazione della funzione di hash unidirezionale) e per lo svolgimento delle opportune verifiche circa la qualità e la rispondenza alle esigenze della ricerca dei dati pseudonimizzati così ottenuti, sotto l'esclusivo controllo del titolare del trattamento. Al termine di queste attività i dati di tipo A saranno cancellati, e quindi cesserà il periodo di conservazione.
- I dati di tipo B (vedi *infra*, Granularità del trattamento) saranno conservati per quanto opportuno e necessario alle finalità del progetto di ricerca, anche con riferimento alle fasi ulteriori (oltre il termine di conclusione delle attività ufficiali), quali ad esempio la diffusione e la discussione dei risultati del progetto di ricerca. In ogni caso, la diffusione e la discussione dei dati avverrà con modalità tali da garantire l'anonimato degli interessati dal trattamento. La conservazione dei dati di tipo B non potrà superare il termine di 5 anni dalla data di formale conclusione del progetto.
- Usi ulteriori dei dati di tipo B: il titolare del trattamento potrebbe decidere di conservare e utilizzare i dati di tipo B oltre il termine di chiusura del progetto di ricerca ACOI e l'ulteriore termine di conservazione di cinque anni, già preventivato, qualora si concretizzassero opportunità di impiego di tali dati per finalità di ricerca e sviluppo omogenee rispetto a quelle che ne hanno giustificato la raccolta e la conservazione iniziale (quali, a titolo di esempio, ulteriori finanziamenti, attivazione di partnership di ricerca, approvazione di progetti di ricerca con il medesimo o analogo oggetto, etc.); in tali casi, il titolare del trattamento provvederà a informare preventivamente gli interessati attraverso specifiche inserzioni sul proprio sito internet e su quelli dei singoli progetti eventualmente attivati, ciò anche al fine di consentire agli interessati, nel rispetto del principio di correttezza e trasparenza, l'esercizio dei diritti loro spettanti in base al Regolamento (art. 15 e ss.)

- **Frequenza della raccolta:** il Progetto ACOI consiste nell'esecuzione di attività scientifica, di sperimentazione e di studio; pertanto il trattamento dei dati avverrà in modo puntuale e non ripetuto

nel tempo. In altre parole, l'obiettivo dell'attività è sperimentare *una tantum* la tecnica di analisi (così da testarne caratteristiche, efficacia, limiti, etc.), e non di ripetere nel tempo ed in termini routinari tale operazione.

- **Granularità del trattamento:** I dati in chiaro (dati di tipo A) sono raccolti e memorizzati presso il titolare e sono utilizzati per ricostruire le reti di interessi che fanno capo ai soggetti che compongono il campione. Una volta ricostruite le reti di interessi, i dati di tipo A (i codici fiscali) sono trattati a fini della loro pseudonimizzazione (tramite procedura di cifratura hash unidirezionale), generando così i dati di tipo B. I dati di tipo B sono i dati su cui il responsabile del trattamento effettua le operazioni di analisi, valutazione e confronto (ai fini della evidenziazione di eventuali profili di rischio di conflitto con gli interessi pubblici perseguiti). I dati di tipo A, dopo l'operazione di pseudonimizzazione non sono più necessari per il progetto di ricerca e vengono cancellati.

Pertanto:

I dati di tipo A sono i dati in chiaro utilizzati per effettuare la ricostruzione e la mappatura delle reti di interessi personali (trattamenti: raccolta, combinazione, e – successivamente – pseudonimizzazione).

I dati di tipo B sono utilizzati per realizzare l'analisi e il confronto con gli interessi pubblici che caratterizzano l'esercizio della funzione (trattamenti: visualizzazione; confronto; evidenziazione). L'analisi avviene verificando la capacità della mappatura, in combinazione con la categorizzazione e il confronto con gli interessi pubblici, di evidenziare situazioni potenziali di rischio di conflitto d'interessi (red flag).

Le informazioni sono raccolte ed elaborate esclusivamente per le finalità del progetto di ricerca ACOI, e conservate per il tempo strettamente necessario a formulare la verifica e validazione del sistema. I dati sono sottoposti ad analisi finalizzate a verificare profili di incompatibilità tra gli interessi personali così evidenziati, nel percorso di ricerca, e lo svolgimento delle specifiche funzioni pubbliche affidate

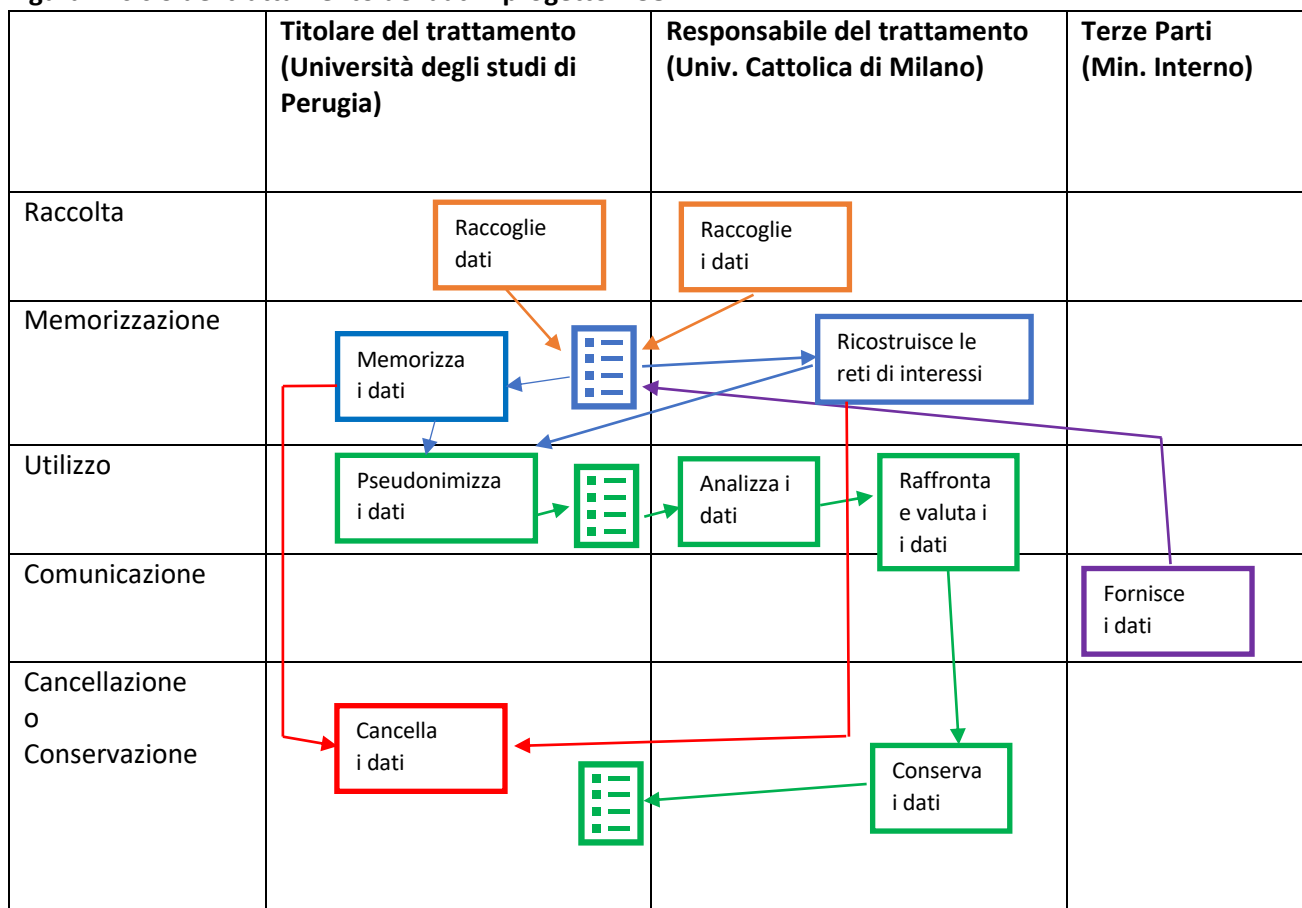
- **Localizzazione del trattamento:** Università degli Studi di Perugia, Università Cattolica del Sacro cuore di Milano

- **Destinatari dei dati:** Responsabile del trattamento, Università Cattolica del Sacro Cuore

- **Descrizioni delle operazioni di trattamento, comprese quelle funzionali allo scopo**

Il ciclo di vita del trattamento dei dati è strettamente funzionale alle finalità di sperimentazione, ricerca e analisi.

Figura 1: ciclo del trattamento dei dati – progetto ACOI



Legenda:

	Dati in chiaro raccolti da sezioni Amministrazione trasparente	Dati di tipo A
	Dati in chiaro comunicati dal Ministero dell'Interno (fonte ANPR)	
	Dati memorizzati in chiaro	Dati di tipo B
	Dati pseudonimizzati (cifatura tramite hash)	
	Dati cancellati (dopo l'operazione di cifatura)	Dati di tipo A

Ciclo: I dati in chiaro (dati di tipo A) sono raccolti, memorizzati e trattati presso il titolare e il responsabile. Il titolare raccoglie e memorizza i dati, mentre il responsabile del trattamento effettua le operazioni di combinazione volte a ricostruire le reti di interessi personali.

Una volta ricostruire le reti di interessi, i dati personali ivi presenti sono oggetto di pseudonimizzazione ad opera del Titolare del trattamento, tramite procedura crittografica unidirezionale di hash. Vengono così generati i dati di tipo B (pseudononimizzati). I dati di tipo B sono i dati su cui il responsabile del trattamento effettua le operazioni analisi e raffronto (ai fini della verifica dell'eventuale situazione di potenziale conflitto d'interesse).

I dati di tipo A sono utilizzati per la ricostruzione delle reti di interessi (trattamento: combinazione, matching). Una volta ricostruite le reti di interessi, ed effettuata l'operazione di pseudonimizzazione, tali dati in chiaro non sono più necessari per il progetto di ricerca, e vengono cancellati.

I dati di tipo B sono utilizzati per l'analisi e per il confronto con gli interessi pubblici che caratterizzano l'esercizio della funzione (trattamento: analisi confronto, evidenziazione). L'analisi avviene verificando la capacità della mappatura, in combinazione con la categorizzazione e il confronto con gli interessi pubblici, di evidenziare situazioni potenziali di rischio di conflitto d'interessi (**red flag**).

Le informazioni sono raccolte ed elaborate esclusivamente per le finalità del progetto di ricerca ACOI, e conservate per il tempo strettamente necessario a formulare la verifica e validazione del sistema. I dati sono sottoposti ad analisi finalizzate a verificare profili di incompatibilità tra gli interessi personali così evidenziati, nel percorso di ricerca, e lo svolgimento delle specifiche funzioni pubbliche affidate.

È importante ribadire che tali trattamenti:

- a) sono esclusivamente funzionali agli scopi di ricerca e sperimentazione del Progetto, il quale mira principalmente a determinare quali indicatori o combinazioni degli stessi possono segnalare potenziali conflitti di interesse;
- b) che le eventuali situazioni individuate non costituiscono di per sé conflitto, ma al più situazioni di anomalia (alla stregua di **red flag**) da valutare in modo più approfondito;
- c) che è esclusa ogni comunicazione all'esterno e o la disseminazione dei dati personali (anche se pseudonimizzati) così raccolti e trattati. Infatti, i risultati della ricerca saranno diffusi e discussi esclusivamente in forma aggregata ed anonima (es. "l'indicatore X è associato a N casi di anomalia potenzialmente riconducibile a un conflitto di interessi", oppure "il Z% dei soggetti analizzati ha riportato un valore anomalo per l'indicatore W"), e secondo modalità che escludono l'identificazione degli interessati;
- d) che tutte queste operazioni avvengono su dati già pseudonimizzati (dati di tipo B), e pertanto non evidenziano informazioni riconducibili a persona identificate;
- e) che i dati personali in chiaro, una volta effettuata la ricostruzione delle reti di interessi, non sono più necessari alle finalità del progetto di ricerca, e vengono cancellati.

➤ **Descrizione degli asset (hw, sw e archivi elettronici, componenti di rete, modelli o archivi cartacei, persone)**

- Memoria locale presso il Titolare del trattamento per la conservazione ed il trattamento dei dati di tipo A
- Memoria in cloud presso il Responsabile del trattamento per la conservazione ed il trattamento dei dati di tipo B
- Software per la memorizzazione e il trattamento dei dati di tipo A e di tipo B.

➤ **I dati sono necessari per le finalità perseguite?**

Il requisito della necessità del trattamento – secondo consolidata giurisprudenza della Corte di giustizia (si vedano, ex multis, le cause C-526/06, C-73/10, C-439/19) – sussiste quando l'obiettivo di interesse pubblico preso in considerazione non può ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi, mezzi che non prevedano il trattamento dei dati personali preso in considerazione.

Nel caso del progetto di ricerca ACOI, come detto, il trattamento è funzionale all'esecuzione dei compiti del Titolare, in quanto **compiti di interesse pubblico** (vedi qui: <https://acoi.scipol.unipg.it/basi-di-liceita-del-trattamento/>).

Il progetto di ricerca intende studiare condizioni, limiti, caratteristiche e opportunità di una soluzione di verifica delle dichiarazioni di assenza di conflitto d'interesse, mediante la ricostruzione della mappa degli interessi che fanno capo al soggetto dichiarante, in accordo con lo schema normativo del conflitto d'interessi. **Tale finalità richiede necessariamente il trattamento di dati personali** (del dichiarante e dei parenti entro il quarto grado, in particolare), dal momento che solo mediante le informazioni che si

riferiscono alla persona identificata è possibile individuare quali sono gli interessi (personali, economici, commerciali, finanziari) che fanno capo a tale persona (colui che presenta la dichiarazione di assenza di conflitto d'interessi), così da poterli mettere a confronto ed in relazione con le finalità e gli interessi pubblici, e così da verificare poi la sussistenza o meno di situazioni, anche potenziali, di conflitto. La ricostruzione della mappa degli interessi va effettuata anche con riferimento ai parenti entro il 2° grado di parentela poiché la fattispecie del conflitto d'interessi, così come individuata dalla legge, ha questa estensione: cfr. l'art. 7 del dpr 63/2013, recante Codice di comportamento dei dipendenti pubblici). Tale finalità non può essere perseguita in modo altrettanto efficace mediante altri mezzi, che non prevedano il trattamento dei dati personali. Di conseguenza, il trattamento dei dati personali indispensabili a individuare, mappare e verificare il conflitto d'interessi risulta necessario per il perseguimento della finalità di interesse pubblico che consiste nello svolgimento della funzione istituzionale di interesse pubblico di ricerca scientifica in capo alle università coinvolte nel progetto, e come tale integra il presupposto di liceità del trattamento dei dati personali (vedi qui <https://acoi.scipol.unipg.it/basi-di-liceita-del-trattamento/>).

Con riguardo alla **minimizzazione dei dati**, affinché siano adeguati, pertinenti e non eccedenti quelli necessari alla verifica degli scenari di rischio, come identificati nel corso del progetto, è insito nei rischi della ricerca la possibilità di raccogliere accidentalmente informazioni eccedenti, in fase di raccolta delle informazioni. E' pertanto previsto di provvedere all'immediata cancellazione delle informazioni che risultino eccedenti, via via che si perviene ad individuare il set di dati necessari per le mappature individuate come output di progetto.

Sempre ai fini della minimizzazione, **nel rispetto di quanto prescritto dall'art. 89, par. 1 del GDPR**, i dati personali necessari per lo svolgimento dello studio **sono previamente trattati in modo da ottenerne la pseudonimizzazione**.

➤ **Informativa all'interessato in termini chiari e modalità trasparenti, esercizio dei diritti**

La mole dei dati personali coinvolti nel trattamento (e quindi dei soggetti interessati) è di circa 500 interessati in quanto soggetti esercenti funzioni pubbliche, cui si aggiungono una stima di circa altre 2000/2500 interessati (soggetti legati da legame di parentela con i soggetti esercenti funzioni pubbliche), per un totale di circa 2500/3000 interessati dal trattamento. La comunicazione diretta ai singoli interessati risulterebbe pertanto gravosa sotto il profilo della gestione, anche tenuto conto del (limitato) budget di progetto e delle risorse disponibili. Inoltre, occorre tenere conto che, come evidenziato nella DPIA, i rischi derivanti dal trattamento sono ridotti al minimo, dal momento che le fasi più delicate del trattamento (analisi, valutazione e confronto, al fine di evidenziare le situazioni di rischio di conflitto di interessi) sono effettuate su dati già pseudonimizzati. Inoltre, dopo la fase di ricostruzione delle reti di interessi che fanno capo agli interessati, i dati in chiaro sono (come detto) prima pseudonimizzati (e su tali dati pseudonimizzati vengono effettuate le successive fasi di analisi), e subito dopo cancellati (come dati in chiaro). Ciò comporta che l'esigenza degli interessati di essere raggiunti dall'informativa tramite comunicazione personale appare alquanto mitigata da tali misure. Pertanto, ai sensi dell'art. 14, par. 5, lett. b) del GDPR, e dell'art. 6, comma 3 delle "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica", di cui all'allegato 1 della delibera del Garante per la protezione dei dati personali n. 515 del 19 dicembre 2018, tenuto conto della misura proporzionata tra onere di gestione dell'informativa ed esigenze di tutela dei diritti degli interessati dai rischi, l'informativa sarà resa nota mediante **idonee forme di pubblicità**. La forma di pubblicità individuata è la pubblicazione sul sito del titolare del trattamento, reperibile all'indirizzo <https://acoi.scipol.unipg.it/>

➤ **Misure di protezione e sicurezza rispetto ai trattamenti illegittimi, perdita di dati, condivisione di dati con terze parti**

Pseudonimizzazione: Il trattamento dei dati ai fini della ricerca (analisi e confronto delle reti di interessi personali, ai fini della individuazione di **red flag** cfr. Figura n. 1) avviene su dati pseudonimizzati, tramite procedura crittografica “hash” unidirezionale. Tale soluzione costituisce già una misura di sicurezza, dal momento che attenua il rischio derivante dall’eventuale dispersione accidentale, colposa o dolosa dei dati, in quanto la pseudonimizzazione rende non identificabili gli interessati al trattamento. I dati personali in chiaro, una volta ricostruire le reti di interessi ed effettuata l’operazione di pseudonimizzazione, vengono cancellati. Anche in questo caso, ciò comporta un aumento del tasso di sicurezza dei trattamenti, dal momento che il tempo in cui i dati personali sono raccolti, memorizzati e trattati in chiaro è quello strettamente necessario alla ricostruzione delle reti di interessi. Dopodiché, i dati in chiaro vengono cancellati. Il rischio di una dispersione accidentale o di un furto è così oggetto di attenuazione, poiché la finestra di opportunità è notevolmente ridotta.

Descrizione degli asset

- Memoria locale presso il Titolare del trattamento per la conservazione ed il trattamento dei dati di tipo A
- Memoria in cloud presso il Responsabile del trattamento per la conservazione ed il trattamento dei dati di tipo B
- Software per la memorizzazione e il trattamento dei dati di tipo A e di tipo B.

Controllo degli accessi logici

Accesso ai dati di tipo A: l’accesso ai dati in formato granulare è consentito al solo Titolare del Trattamento. L’accesso è protetto mediante sistemi di autenticazione (password modificata ogni 4 mesi).

Accesso ai dati di tipo B: l’accesso è consentito al responsabile del trattamento e agli addetti al trattamento (utenti autorizzati, UA). Verranno implementati mezzi di autenticazione. Solo agli UA verranno forniti un nome utente e una password temporanea per l’accesso allo strumento. Gli UA sostituiranno la password temporanea dopo il primo accesso. Le password avranno le seguenti caratteristiche: saranno composte da un minimo di otto caratteri; dovranno essere rinnovate ogni 4 mesi; dovranno essere rinnovate se c’è il minimo rischio che possano essere state compromesse; dovranno includere almeno tre di quattro tipi di caratteri (es. lettere maiuscole, lettere minuscole, numeri e caratteri speciali); quando si cambia una password, le ultime due password non potranno essere riutilizzate.

Controllo degli accessi fisici

Accesso ai dati di tipo A: l’accesso alla memoria fisica in cui sono conservati in cui sono di tipo A è consentito al solo Titolare del Trattamento. L’accesso alla memoria fisica è protetto mediante sistema di autenticazione biometrico.

Accesso ai dati di tipo B: l’accesso ai locali in cui sono conservati e gestiti i dati di tipo B è consentito solo al personale che svolge attività di ricerca presso il responsabile del trattamento.

Gestione del personale

Il personale coinvolto nell'attività di ricerca è affiliato ad un ente di ricerca, ed è caratterizzato da un profilo professionale che assicura una spiccata sensibilità per le esigenze di tutela dei dati, sia nel corso della sperimentazione che successivamente alla sua conclusione. Il personale addetto al trattamento dei dati personali, sia quelli di tipo A che quelli di tipo B, è informato per iscritto dei doveri di rispetto della disciplina a tutela dei dati personali e dei doveri deontologici specifici connessi al trattamento dei dati personali nell'ambito delle attività di ricerca scientifica (regole deontologiche del Garante privacy). Il personale specificamente addetto al trattamento dei dati personali sottoscrive una dichiarazione di impegno al rispetto delle norme a tutela dei dati personali, e delle regole deontologiche specifiche per il trattamento dei dati personali nell'ambito della ricerca scientifica.

Sicurezza dell'hardware e del software

Conservazione dei dati di tipo A: l'hardware in dotazione al titolare del trattamento è presidiato da accessi malevoli dall'esterno mediante sistemi di sicurezza adeguati e aggiornati. Il software e il sistema di memorizzazione impiegato assicura che i dati sono conservati esclusivamente in memoria locale.

Conservazione dei dati di tipo B: i dati di tipo B (pseudonimizzati) sono conservati e gestiti su GoogleCloud: il contratto di servizio consente la conservazione dei dati nel datacenter locale (Torino), ciò che impedisce che i dati possano transitare in paesi terzi.

Sicurezza dei canali informatici

I flussi di scambio dei dati personali tra il titolare del trattamento, responsabile del trattamento e terzi (Ministero dell'Interno) avviene secondo quanto indicato nella Figura 1. Con riferimento ai dati di tipo A, lo scambio (che avviene esclusivamente dal responsabile del trattamento verso il titolare del trattamento) è operato mediante file protetti da sistemi di autenticazione. I file sono trasmessi mediante i canali di posta elettronica istituzionale; le credenziali per l'autenticazione sono comunicate separatamente e su canale sicuro e crittografato. Lo scambio di dati personali in chiaro (dati di tipo A) tra il Titolare del trattamento e il Ministero dell'Interno avviene mediante le medesime modalità: file protetti da sistema di autenticazione, credenziali per l'autenticazione comunicate separatamente, su canale sicuro e crittografato. La password è modificata in occasione di ciascun invio.

I dati di tipo B sono scambiati mediante file protetti da sistema di autenticazione username/password.

Nel registro dei trattamenti sono registrati gli scambi di dati di tipo A.

I dati sono scambiati adottando le misure di sicurezza accessorie più opportune per evitare la dispersione accidentale o il furto di tali dati.

Tempestiva ed efficace cancellazione dei dati personali

Dati di tipo A: In esito alle operazioni connesse alla pseudonimizzazione, i dati personali di tipo A saranno definitivamente cancellati.

Trasferimento dei dati verso paesi terzi (extra UE ed organizzazioni internazionali)

Non è previsto il trasferimento dei dati al di fuori dell'Unione europea

Comunicazione tempestiva delle violazioni di dati

Il titolare ed il responsabile del trattamento operano con la opportuna diligenza al fine di monitorare le infrastrutture e i processi mediante i quali sono compiute le operazioni di trattamento (quali conservazione, comunicazione, combinazione, analisi). Comunicano tempestivamente al dpo di struttura e al Garante privacy ogni significativa violazione dei dati (quali: l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;

il furto o la perdita di dispositivi informatici contenenti dati personali; la deliberata alterazione di dati personali; l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.; la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità; la divulgazione non autorizzata dei dati personali), comunque **entro 48 ore dal momento in cui ne è venuto a conoscenza**.

Valutazione delle minacce

Le minacce possono essere identificate in relazione a circostanze quali:

A. il contesto

B. gli strumenti

C. il comportamento umano

D. le conseguenze, in termini di impedimenti per gli interessati di esercitare un diritto o di subire un pregiudizio o danno

Accesso illegittimo dei dati (vs. Riservatezza)		
1	Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	Tipologia dati A: la conoscenza delle informazioni relative a rapporti familiari, interessi economici e interessi patrimoniali potrebbero determinare rischi per l'integrità degli interessi finanziari ed economici degli interessati, che potrebbero subire un danno reputazionale o la minaccia di soggetti interessati ad appropriarsene ed utilizzarli in modo illecito. Tipologia di dati B: i dati relativi alla mappatura degli interessi in capo ai soggetti interessati sono analizzati in forma di dati pseudonimizzati. Pertanto, i rischi potenziali derivanti dalla conoscenza della mappa (rischi per l'integrità del patrimonio, rischi di profilazione, rischi per l'incolumità anche fisica degli interessati e dei familiari più stretti) appaiono mitigati in modo molto significativo, dal momento che la cifratura mediante funzione di hash unidirezionale rende non identificabili i soggetti.
2	Quali sono le principali minacce che potrebbero concretizzare il rischio?	Tipologia dati A: i dati sono conservati e trattati ai fini della ricostruzione delle mappe/reti di interessi. Le minacce sono rappresentate dal furto mediante accesso diretto alla memoria fisica su cui sono conservati. Tipologia dati B: i dati (pseudonimizzati) sono conservati e trattati dal responsabile del trattamento e dagli operatori da questi espressamente autorizzati. Le minacce sono costituite da: - Dispersione malevola da parte del personale addetto al trattamento - Furto
3	Quali sono le fonti di rischio?	Tipologia dati A: fonti esterne; fonti interne (dispersione accidentale)

		Tipologia di dati B: fonti interne: addetti al trattamento fonti esterni: soggetti esterni
4	Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	Tipologia dati A: 1) il controllo esclusivo da parte del titolare del trattamento sulla memoria fisica dove sono conservati i dati in formato granulare, in luogo sicuro, non aperto al pubblico e il cui accesso è presidiato (la memoria è ospitata nei locali dell'Università, soggetti a custodia, vigilanza e dentro stanze chiuse a chiave), contribuisce in modo decisivo ad attenuare il rischio di furto. Inoltre, l'accesso ai dati è presidiato anche tramite strumenti di autenticazione. 2) la durata limitata della conservazione di questa tipologia di dati contribuisce ad attenuare il rischio. Infatti, una volta effettuata il trattamento che consente di ricostruire le reti di interessi, i dati personali sono oggetto delle operazioni di pseudonimizzazione, mentre i dati personali in chiaro, subito dopo, sono cancellati e non più conservati. Tipologia dati B: i dati sono pseudonimizzati. Questa misura abbatta considerevolmente il rischio connesso all'accesso illegittimo ai dati. Inoltre, gli addetti che trattano i dati sono solo quelli autorizzati allo scopo, e sono sottoposti a specifici impegni deontologici connessi al trattamento alla disponibilità dei dati.
5	Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali?	Con riferimento ai dati di tipo A, il rischio stimato è Alto. Con riferimento ai dati di tipo B, il rischio stimato è medio.
6	Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio?	Con riferimento ai dati di tipo A, il rischio stimato è basso. Con riferimento ai dati di tipo B, il rischio stimato è medio-basso.
7	Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali, tenuto conto delle misure pianificate?	Tenuto conto delle misure di mitigazione applicate, con riferimento ai dati di tipo A, il rischio stimato è basso. Con riferimento ai dati di tipo B, il rischio stimato è medio-basso.
8	Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Tenuto conto delle misure di mitigazione applicate, con riferimento ai dati di tipo A, il rischio stimato è basso. Con riferimento ai dati di tipo B, il rischio stimato è basso

Modifiche indesiderate dei dati (vs Integrità)		
1	Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?	Tipologia dati A: la compromissione dell'integrità dei dati potrebbe comportare una rappresentazione non veritiera delle informazioni relative ai soggetti interessati) informazioni relative a rapporti familiari, interessi economici e interessi patrimoniali),

		con possibile, conseguente impatto sul diritto all'identità, alla reputazione, nonché sul diritto all'integrità del patrimonio e della sfera fisica e psichica. Tipologia di dati B: i dati sono pseudonimizzati, pertanto i rischi connessi alla compromissione dell'integrità dei dati sono ridotti, in quanto le informazioni non corrette, alterate non sarebbero riconducibili a soggetti identificati o identificabili. Impatto ridotto.
2	Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?	Tipologia dati A: errori materiali da parte del Titolare del trattamento. Errori materiali nella estrazione e raccolta dei dati. Tipologia di dati B: (i dati sono pseudonimizzati) errori materiali nell'effettuazione delle operazioni di trattamento (combinazione, analisi)
3	Quali sono le fonti di rischio?	Tipologia dati A: interne; esterne Tipologia di dati B: interne
4	Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	Tipologia dati A: limitazione delle operazioni di trattamento; sottoscrizione da parte del titolare del trattamento degli specifici impegni deontologici relativi al trattamento dei dati personali oggetto della ricerca Tipologia di dati B: formazione e sensibilizzazione specifiche e dedicate; istruzioni specifiche agli addetti autorizzati al trattamento; sottoscrizione da parte del titolare del trattamento degli specifici impegni deontologici relativi al trattamento dei dati personali oggetto della ricerca
5	Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali?	Con riferimento ai dati di tipo A, il rischio stimato è Alto. Con riferimento ai dati di tipo B, il rischio stimato è medio.
6	Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio?	Con riferimento ai dati di tipo A, il rischio stimato è basso. Con riferimento ai dati di tipo B, il rischio stimato è basso.
7	Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali, tenuto conto delle misure pianificate?	Tenuto conto delle misure di mitigazione applicate, con riferimento ai dati di tipo A, il rischio stimato è medio-basso. Con riferimento ai dati di tipo B, il rischio stimato è basso.
8	Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Tenuto conto delle misure di mitigazione applicate, con riferimento ai dati di tipo A, il rischio stimato è basso. Con riferimento ai dati di tipo B, il rischio stimato è basso

Perdita dei dati (vs Disponibilità)		
1	Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?	Tipologia dati A: la conoscenza accidentale delle informazioni relative a rapporti familiari, interessi economici e interessi patrimoniali potrebbe determinare alcuni rischi (non sistematici, tuttavia) per l'integrità degli interessi finanziari ed economici degli interessati, che potrebbero subire la minaccia di soggetti interessati ad appropriarsene in modo illecito. Tipologia di dati B: i dati relativi alla ricostruzione della mappatura degli interessi in capo ai soggetti interessati sono formati e trattati a partire da dati personali pseudonimizzati. Pertanto, i rischi potenziali derivanti dalla conoscenza accidentale della mappa (rischi per l'integrità del patrimonio, rischi di profilazione, rischi per l'incolumità anche fisica degli interessati e dei familiari più stretti) appaiono mitigati in modo molto significativo, dal momento che la funzione di hash rende non identificabili i soggetti.
2	Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?	Tipologia dati A: sostanzialmente assenti (l'eventuale distruzione o blocco della memoria fisica non determinerebbe la dispersione dei dati, ma semmai l'impossibilità di utilizzarli, o la relativa cancellazione) Tipologia di dati B: errori materiali accidentali da parte del personale addetto al trattamento; malf funzionamento dei sistemi.
3	Quali sono le fonti di rischio?	Tipologia dati A: interne Tipologia di dati B: interne, esterne (malf funzionamento)
4	Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	Tipologia dati A: qualità della memoria locale in cui sono conservati i dati Tipologia di dati B: formazione e sensibilizzazione specifiche e dedicate; istruzioni specifiche agli addetti autorizzati al trattamento; sottoscrizione da parte del titolare del trattamento degli specifici impegni deontologici relativi al trattamento dei dati personali oggetto della ricerca; qualità e verifiche della funzionalità dei sistemi in uso.
5	Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali?	Con riferimento ai dati di tipo A, il rischio stimato è Alto. Con riferimento ai dati di tipo B, il rischio stimato è medio-basso.
6	Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio?	Con riferimento ai dati di tipo A, il rischio stimato è medio-basso. Con riferimento ai dati di tipo B, il rischio stimato è basso.

7	Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali, tenuto conto delle misure pianificate?	Tenuto conto delle misure di mitigazione applicate, con riferimento ai dati di tipo A, il rischio stimato è basso. Con riferimento ai dati di tipo B, il rischio stimato è basso.
8	Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	Tenuto conto delle misure di mitigazione applicate, con riferimento ai dati di tipo A, il rischio stimato è basso. Con riferimento ai dati di tipo B, il rischio stimato è basso

Misure di mitigazione

Le misure di mitigazione del rischio assunte sono le seguenti:

- Pseudonimizzazione dei dati personali, tramite crittografia unidirezionale di hash. Questa misura abbatta in modo significativo i rischi connessi al trattamento dei dati in esecuzione del progetto di ricerca, dal momento che i dati pseudonimizzati non contestano l'identificazione dell'interessato.
- Conservazione dei dati personali "in chiaro" per il solo tempo necessario ad applicare la misura di pseudonimizzazione; dopodiché i dati sono cancellati.
- Personale addetto al trattamento appositamente istruito sui rischi e le modalità di corretta gestione dei dati e dei trattamenti, in accordo con le regole deontologiche specifiche per l'attività di ricerca scientifica
- Accessi logici limitati ai soli addetti alle operazioni di trattamento, mediante sistemi di sicurezza (accesso tramite password)
- Accesso fisico ai locali dove sono conservati e gestiti i dati precluso a soggetti estranei all'attività del gruppo ricerca.
- Aggiornamento dei software in uso per il trattamento dei dati personali
- Condivisione e chiarezza della policy di trattamento dei dati con tutti il team di ricerca; condivisione degli obblighi deontologici specifici connessi allo svolgimento dell'attività di ricerca
- Definizione corretta e completa degli atti di nomina a Responsabile del trattamento, con verifica dell'atto di nomina dei sub-responsabili.

Valutazione del rischio residuo

Alla luce della valutazione dell'impatto delle misure di mitigazione attuate, il rischio residuo risulta come da tabella seguente:

Fattori di rischio	Rischio residuo
Accesso illegittimo dei dati (vs. Riservatezza)	Basso
Modifiche indesiderate dei dati (vs Integrità)	Basso
Perdita dei dati (vs Disponibilità)	Basso