

Soggetti vulnerabili e Privacy

nel campo della ricerca scientifica, ai sensi del considerando 75 GDPR, del WP 248 Gruppo di lavoro articolo 29 e delle regole deontologiche per trattamenti ai fini statistici o di ricerca scientifica

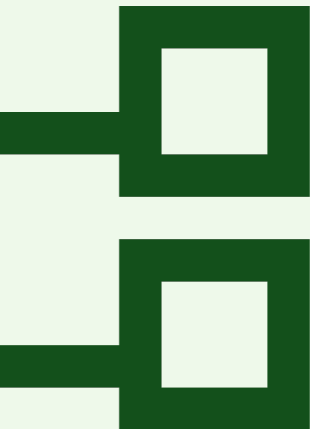
Giugno 2025

Questo documento è stato redatto Himmel Advisors. È vietata qualsiasi riproduzione o copia, totale o parziale, senza il permesso esplicito di Himmel Advisors

Ulteriori informazioni
www.himmeladvisors.it

Chi sono i soggetti vulnerabili?

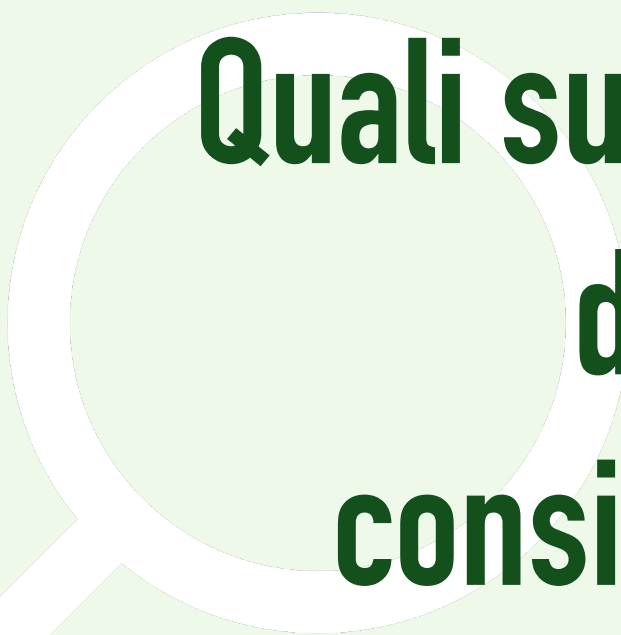
Cfr. Considerando 75 GDPR



categoria di soggetti eterogenea cui la normativa in materia di Data Protection destina particolari tutele e garanzie in ragione della loro particolare condizione di suscettibilità al rischio inerente alle attività di trattamento svolte dal titolare o dal responsabile (es. in occasione della raccolta, gestione ed elaborazione di dati sensibili nell'ambito di un progetto di ricerca scientifica)



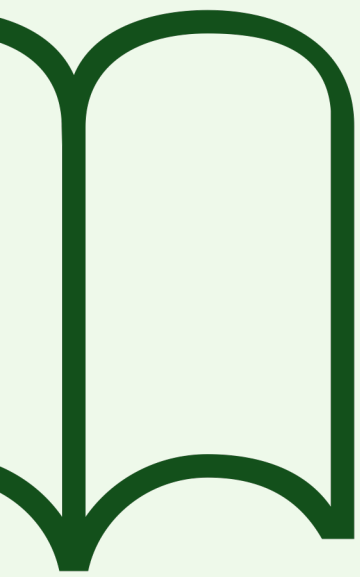
Nella presente pubblicazione si dichiara che i termini "interessati" o "interessate" sono utilizzati indifferentemente in entrambi i generi, al fine di garantire l'equità e la parità di rappresentanza linguistica, nel rispetto delle norme di redazione giuridica e di buona prassi inclusiva



**Quali suggerimenti
da tenere in
considerazione?**



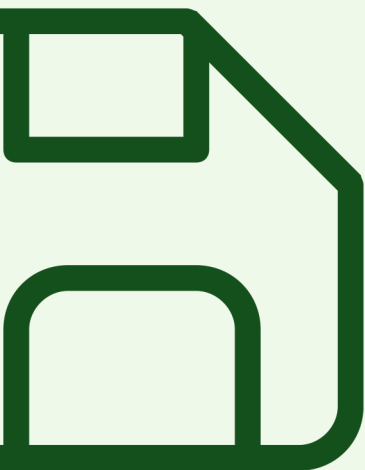
Data Protection Impact Assessment (DPIA)



«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 effettua, prima di procedere al trattamento, una DPIA (ex art. 35 GDPR)

Una singola DPIA può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi»

Identificazione tipologia dati e soggetti



In fase di elaborazione della DPIA è doveroso **identificare la tipologia di dati personali oggetto di trattamento ed i soggetti a cui si riferiscono** al fine di determinare l'impatto del trattamento dal punto di vista privacy



Identificare dati e soggetti è un'attività propedeutica all'attività di ricerca e per la conduzione della DPIA poiché, in fase di svolgimento del progetto, l'eventuale raccolta di dati (anche di categorie diverse di soggetti) comporterebbe la revisione della DPIA

Obbligo di trasparenza



È doveroso che il team di ricerca metta a disposizione dei partecipanti ad un progetto tutti gli elementi riguardanti il trattamento dei dati personali sin dall'inizio della partecipazione. Il partecipante ha il diritto di sapere chi, come e perché vengono trattati i dati per finalità di ricerca scientifica



La trasparenza non si traduce nella pubblicazione dell'informativa privacy ma nel dare la possibilità agli interessati di conoscere e comprendere il progetto a 360°

Consenso al trattamento dei dati personali



È necessario che tutti i partecipanti ad un progetto di ricerca abbiano fornito, liberamente, un consenso (ai sensi dell'art. 6 o 9 GDPR). Il **consenso non è una mera formalità** ma un modo per verificare che i partecipanti abbiano compreso gli obiettivi del progetto spiegando come verranno utilizzati i loro dati



In fase di raccolta del consenso, i ricercatori devono rendersi disponibili per aiutare a comprendere gli obiettivi del progetto a tutti i potenziali soggetti partecipanti

Consenso al trattamento dei dati personali (i)



Alcuni soggetti vulnerabili potrebbero trovarsi nell'impossibilità di esprimere un valido consenso in applicazione del GDPR e della normativa di settore, in quanto privi della capacità di intendere e di volere. In tali ipotesi, è imprescindibile individuare correttamente la figura competente ad agire in nome e per conto del partecipante, quale, ad esempio, i genitori o altri soggetti esercitanti la responsabilità genitoriale o tutoria, ai fini del rilascio del consenso obbligatorio ai sensi delle normative applicabili.



Va documentato il consenso fornito da parte del soggetto autorizzato e legittimato e fornita un'informativa privacy (ex art. 13 GDPR) anche a tale soggetto in quanto vengono trattati i dati dello stesso

Misure di sicurezza fisiche, tecniche ed organizzative (MFTO)



Nel contesto del trattamento di dati personali di soggetti vulnerabili, è essenziale considerare attentamente il rischio intrinseco associato a tali attività. Questo richiede un'analisi dettagliata basata sull'impatto potenziale delineato nel considerando n. 75 del GDPR. Tale considerazione evidenzia la possibilità che il trattamento possa causare danni fisici, materiali o immateriali, in particolare quando coinvolge dati di persone fisiche vulnerabili, come i minori. È necessario articolare la DPIA concentrandosi su minacce e impatti specifici al fine di adottare misure adeguate per mitigare tali rischi

Le MFTO devono essere identificate e implementate prima dell'inizio del trattamento dei dati previsto. Tali misure devono essere rispettate dal ricercatore per l'intera durata del progetto, inclusa la fase successiva all'anonimizzazione o alla cancellazione dei dati, che potrebbe avvenire a seguito della pubblicazione dei risultati. Questo approccio garantisce che la protezione dei dati personali sia mantenuta costantemente e non venga compromessa in nessuna fase del trattamento

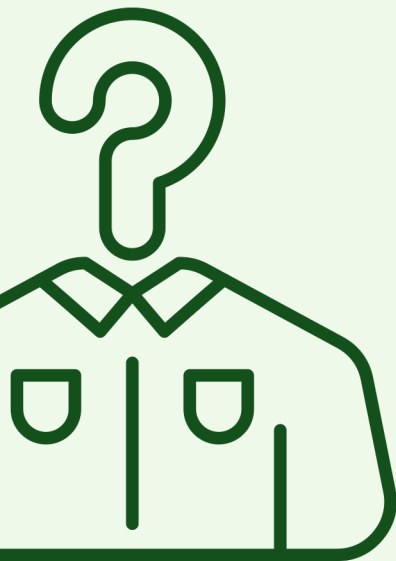
Misure di sicurezza fisiche, tecniche ed organizzative (MFTO)



I ricercatori sono tenuti a sottoscrivere una «dichiarazione di impegno» ai sensi delle «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica». Un'analogha dichiarazione è sottoscritta anche dai soggetti – ricercatori, responsabili e persone autorizzate al trattamento – che fossero coinvolti nel prosieguo della ricerca, e conservata »per circa 5 anni dalla conclusione programmata della ricerca»



(Pseudo)Anonimizzazione




Ove possibile, nell'ambito della ricerca scientifica è necessario implementare **misure ulteriori di sicurezza** per eliminare alcuni elementi che potrebbero consentire di identificare direttamente l'interessato. La pseudonimizzazione è una misura di sicurezza tecnica e una strategia vincente per mitigare i rischi associati al trattamento dei dati personali

La diffusione dei risultati dell'attività di ricerca tramite la raccolta e gestione di dati riconducibili a soggetti vulnerabili deve avvenire, sempre e comunque, in maniera anonima (e non pseudonimizzata)



Attenzione! I dati pseudonimizzati sono «dati personali» in quanto possono essere ricondotti a un soggetto identificabile mediante il ricorso a informazioni supplementari

Archiviazione e accesso limitato



Conservare i dati in luoghi sicuri, utilizzando strumenti di crittografia per prevenire accessi non autorizzati è una delle principali misure di sicurezza da applicare al trattamento di dati personali relativi a soggetti vulnerabili. Tali strumenti devono garantire che i dati siano protetti da accessi non autorizzati durante tutte le fasi di trattamento, dalla raccolta alla conservazione, fino alla eventuale anonimizzazione o cancellazione. La crittografia rappresenta una delle principali tecniche di sicurezza in fase di archiviazione, poiché trasforma i dati in un formato illeggibile senza le chiavi di decrittazione corrispondenti, riducendo sensibilmente il rischio di esposizione in caso di intrusioni o compromissioni dei sistemi. È altresì fondamentale che i dati forniti dai partecipanti siano custoditi in modo accurato e responsabile, adottando procedure di archiviazione che rispettino le best practice di sicurezza informatica, garantendo la protezione della riservatezza, dell'integrità e della disponibilità delle informazioni



L'accesso deve essere rigorosamente limitato al personale strettamente coinvolto nel progetto (i ricercatori autorizzati), e questa autorizzazione deve essere gestita mediante procedure di controllo e tracciabilità, come sistemi di autenticazione forte e registrazione delle operazioni di accesso

Revoca consensi

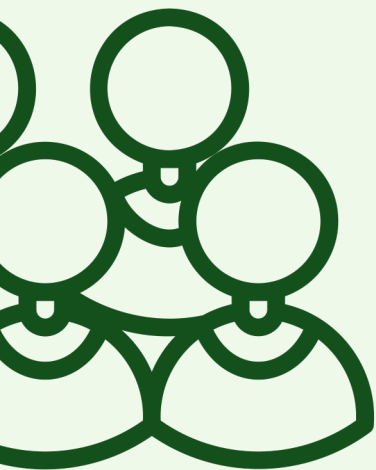


Nel contesto di un progetto di ricerca, si precisa che i partecipanti hanno il diritto di revocare il proprio consenso e di interrompere la partecipazione in qualsiasi momento, prima dell'effettiva finalizzazione del processo di anonimizzazione o della cancellazione dei dati raccolti e trattati. Di fronte a tale richiesta, il titolare del trattamento è obbligato a procedere alla cancellazione dei predetti dati entro e non oltre trenta (30) giorni dalla ricezione della relativa richiesta, garantendo così il rispetto dei principi di tutela dei diritti dell'interessato e di correttezza nel trattamento dei dati personali



I ricercatori sono tenuti a fornire ai partecipanti, al momento della loro adesione al progetto, un'informativa privacy in cui si specificò che questi ultimi hanno il diritto di revocare la propria partecipazione in qualsiasi momento, utilizzando le modalità stabilite dal Titolare, senza che ciò comporti alcuna conseguenza svantaggiosa o inadempimento rispetto alla partecipazione stessa

Comitato Etico

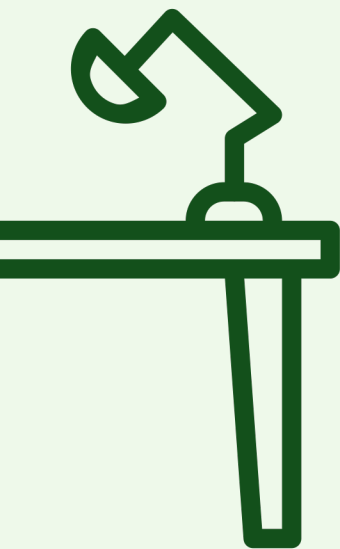


Il ruolo del Comitato Etico nella ricerca scientifica si configura come un elemento fondamentale volto a garantire il rispetto degli standard etici e di tutela dei diritti dei partecipanti allo studio. Pur trattandosi di ambiti distinti – quello dell’etica e quello della protezione dei dati personali – si privilegia un interesse comune, ovvero la salvaguardia della dignità, della sicurezza e dei diritti degli soggetti coinvolti. In particolare, il Comitato Etico esercita un’attività di valutazione e supervisione delle modalità di svolgimento della ricerca, assicurando che siano adottate tutte le misure atte a rispettare i principi di correttezza, equità e trasparenza, anche in conformità con le normative vigenti sulla privacy e sulla protezione dei dati personali.



La sua funzione si traduce, quindi, in una garanzia complessiva a tutela della salute, della dignità umana e dei diritti degli interessati, assicurando che l’attività di ricerca si svolga nel pieno rispetto dei principi etici e normativi di riferimento

Formazione



Il team di ricerca ha l'obbligo di ricevere istruzioni in materia di protezione dei dati personali, principalmente in fase di privacy by design e by default, ovvero in fase di conduzione della DPIA, con particolare attenzione alla natura dei soggetti coinvolti, i quali spesso rivestono caratteristiche di vulnerabilità. Tale consapevolezza implica che i membri del team siano informati e sensibilizzati sul fatto che i dati trattati riguardano soggetti vulnerabili, che richiedono, di conseguenza, misure di protezione e tutela rafforzate e pertinenti, al fine di garantire il rispetto dei principi di riservatezza, integrità e dignità degli interessati



Soggetti vulnerabili e Privacy

nel campo della ricerca scientifica, ai sensi del considerando 75 GDPR, del WP 248 Gruppo di lavoro articolo 29 e delle regole deontologiche per trattamenti ai fini statistici o di ricerca scientifica

Giugno 2025

Questo documento è stato redatto Himmel Advisors e può essere utilizzato esclusivamente per le finalità indicate. È vietata qualsiasi riproduzione o copia, totale o parziale, senza il permesso esplicito di Himmel Advisors.



www.himmeladvisors.it

