La protezione dei dati personali nella ricerca scientifica

Il Regolamento UE 2016/679 (RGPD/GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione dei dati
si applica anche
al trattamento dei dati personali per finalità di ricerca scientifica e statistica e statistica.

La scheda di analisi e dichiarazione d'impegno del progetto di ricerca prevista dalle "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica" (G.U. del 14 gennaio 2019, n. 11) e stilata in conformità agli standard metodologici del pertinente settore disciplinare, è uno strumento utile per documentare le scelte effettuate, esaminare gli aspetti connessi alla protezione dei dati e applicare i principi alla base della normativa in materia di protezione dei dati nella progettazione della ricerca (il modello è stato redatto tenendo conto delle indicazioni del gruppo di lavoro CODAU).

La scheda:

- viene compilata dal responsabile scientifico di ciascun progetto nel caso in cui il progetto di ricerca comporti il trattamento di dati personali;
- è finalizzata a raccogliere le informazioni necessarie per definire le misure da adottare al fine di rendere il trattamento dei dati personali conforme a quanto previsto dalla normativa;
- contiene la dichiarazione d'impegno sottoscritta dal responsabile scientifico e dai ricercatori coinvolti nel progetto;
- viene depositata presso la struttura di afferenza del responsabile del progetto che ne cura la conservazione in forma riservata. La consultazione del progetto è possibile ai soli fini dell'applicazione della normativa in materia di dati personali. La scheda deve essere conservata per cinque anni dalla conclusione programmata della ricerca;
- permette di inserire la ricerca nel Registro dei trattamenti del Dipartimento.

I passaggi fondamentali per redigere la scheda di analisi e, più in generale, per avviare una ricerca a norma di privacy:

LE FASI DEL PROGETTO	**APPROFONDIMENTI E STRUMENTI OPERATIVI**
1. Definire i ruoli dei soggetti che prendono parte allo studio	Se la finalità della ricerca viene raggiunta in collaborazione con un altro Partner (Università, Enti di ricerca) con cui vengono condivisi i dati possono ricorrere casi differenti, solitamente riferibili a tre tipologie di seguito riportate: TITOLARI AUTONOMI; CONTITOLARI; RESPONSABILI ESTERNI. è disponibile il Flowchart per l'applicazione pratica dei concetti di titolare, responsabile e contitolare del trattamento

2. Il rispetto del principio di Accountability	La Responsabilizzazione=accountability consiste nell'insieme delle misure tecniche e organizzative adottate dai titolari e responsabili del trattamento per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento UE. Misure di sicurezza (cfr. all.): - dati pseudonimizzati (non possono più essere attribuiti a un interessato senza utilizzare informazioni aggiuntive, conservate separatamente con misure di protezione adeguate); - dati o documenti crittografati (proteggendo adeguatamente la chiave per la decodifica), anche per la custodia e condivisione/trasmissione. Misure di sicurezza nella ricerca: https://privacy.unipv.it/intranetdologin/misure-di-sicurezza-nella-ricerca/
3. Decidere su base giuridica, informativa, consenso, esercizio dei diritti	Il CONSENSO ex art. 6 lett. a) RGPD deve essere una manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato. Si tratta di una base giuridica utilizzata in maniera preponderante per finalità di ricerca in Italia. Modello di informativa per il trattamento di dati sensibili in un progetto di ricerca
4. Effettuare l'analisi dei rischi per la protezione dei dati personali e DPIA.	Verificare al seguente link se occorre effettuare la Valutazione d'impatto-DPIA: https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto
5. Sottoporre, ove necessario, il progetto al Comitato etico	The Ethics and Data Protection Decision Tree can further support you in identifying and addressing potential ethics issues related to the data processing activities in your project
6. Conservazione dei dati	I dati personali dovrebbero essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. Per la determinazione del periodo massimo di conservazione dei dati personali ai fini della ricerca, occorre tener conto anche delle criticità conseguenti al dover garantire, per tutta la durata di tale periodo, la riservatezza, l'integrità e la disponibilità di tali dati personali, fermo restando che dovrebbero essere anonimizzati appena ciò sia possibile nel contesto della ricerca.

7. In caso di esportazione/importazione di dati personali extra UE occorre applicare le disposizioni previste dalla normativa	I trasferimenti dati extra UE: https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero
8. Compilare il registro delle attività di trattamento	Il registro rappresenta l'elemento centrale per la governance del modello di gestione privacy e viene tenuto in formato elettronico. All'interno della Scuola IUSS sono redatti due Registri: il Registro del Titolare e il Registro del Responsabile (relativo ai trattamenti che l'Università effettua per conto di soggetti esterni).
9. Violazioni di dati personali	Le violazioni di dati personali subite devono essere documentate anche se non notificate all'autorità di controllo e non comunicate agli interessati. Tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del titolare sono tenuti nel caso di una concreta, potenziale o sospetta violazione dei dati personali ad informare dell'incidente il responsabile della struttura (responsabile di servizio, direttore tecnico, segretario di coordinamento etc.) il quale si occuperà, di informare il Titolare del trattamento o un suo delegato mediante la compilazione Modulo di comunicazione di Data Breach.

TRATTAMENTO DI DATI PARTICOLARI PER SCOPI DI RICERCA
Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 (Pubblicate sulla Gazzetta Ufficiale n. 11 del 14 gennaio 2019)

Le regole deontologiche si applicano all´insieme dei trattamenti effettuati per scopi statistici e scientifici –conformemente agli standard metodologici del pertinente settore disciplinare –, di cui sono titolari università, altri enti o istituti di ricerca e società scientifiche, nonché ricercatori che operano nell´ambito di dette università, enti, istituti di ricerca e soci di dette società scientifiche.
Le regole deontologiche non si applicano ai trattamenti per scopi statistici e scientifici connessi con attività di tutela della salute svolte da esercenti professioni sanitarie od organismi sanitari, ovvero con attività comparabili in termini di significativa ricaduta personalizzata sull´interessato, che restano regolati dalle pertinenti disposizioni. La ricerca svolta per questi ultimi scopi è invece soggetta alle disposizioni di carattere generale dedicate all'ambito medico-sanitario.

Adempimenti del Responsabile del progetto:

1. La ricerca è effettuata sulla base di un progetto redatto conformemente agli standard metodologici del pertinente settore disciplinare, anche al fine di documentare che il trattamento sia effettuato per idonei ed effettivi scopi statistici o scientifici.
2. Il progetto di ricerca di cui al comma 1, inoltre:
   a. specifica le misure da adottare nel trattamento di dati personali, al fine di garantire il rispetto delle presenti regole deontologiche, nonché della normativa in materia di protezione dei dati personali;
   b. individua gli eventuali responsabili del trattamento;
   c. contiene una dichiarazione di impegno a conformarsi alle presenti regole deontologiche. Un´analoga dichiarazione è sottoscritta anche dai soggetti – ricercatori, responsabili e persone autorizzate al trattamento – che fossero coinvolti nel prosieguo della ricerca;
3. Il titolare deposita il progetto presso l´università o ente di ricerca o società scientifica cui afferisce, la quale ne cura la conservazione, in forma riservata (essendo la consultazione del progetto possibile ai soli fini dell´applicazione della normativa in materia di dati personali), per cinque anni dalla conclusione programmata della ricerca;
4. Nel trattamento di dati relativi alla salute, i soggetti coinvolti osservano le regole di riservatezza e di sicurezza cui sono tenuti gli esercenti le professioni sanitarie o regole di riservatezza e sicurezza comparabili.

Il Responsabile del progetto inoltre è tenuto a:

1. fornire l'informativa ai soggetti interessati, in modo che sia chiaro se si tratta di attività di ricerca o di tutela della salute;
2. raccogliere il consenso;

Il consenso al trattamento dei dati idonei a rivelare lo stato di salute è, pertanto, di regola necessario. Nel manifestare il proprio consenso ad un'indagine medica o epidemiologica, all'interessato è richiesto di dichiarare se vuole conoscere o meno eventuali scoperte inattese che emergano a suo carico durante la ricerca.
Il consenso dell'interessato non è necessario quando, siano soddisfatte contemporaneamente tutte le condizioni previste nell' art. 110 del D. Lgs. 196/2003:

Art. 110 (Ricerca medica, biomedica ed epidemiologica)

1. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.

2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del regolamento nei riguardi dei trattamenti di cui al comma 1, la rettificazione e l'integrazione dei dati sono annotate senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.

3. se necessario, ottenere il preventivo parere del Comitato etico.

Autorizzazioni generali del Garante
Il Garante per la protezione dei dati personali ha emanato:
- Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016). https://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/9068972#5
- Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016) https://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/9068972#4

Diffusione dei dati
I dati idonei a rivelare lo stato di salute degli interessati, nonché quelli relativi alla vita sessuale e all'origine razziale ed etnica utilizzati per la conduzione dello studio non possono essere diffusi.
I risultati delle ricerche possono essere diffusi in forma aggregata, ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti, anche nell'ambito di pubblicazioni.

Custodia e sicurezza
Sussiste l'obbligo di messa in atto di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR), che comprendono, tra le altre, se del caso:
- la pseudonomizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Vanno prese in considerazione la fase della memorizzazione o archiviazione dei dati (e, eventualmente, di raccolta e conservazione dei campioni biologici), quella successiva di elaborazione delle medesime informazioni e di trasmissione delle stesse a eventuali soggetti esterni che collaborano con la realizzazione della ricerca.
Sono adottati, in particolare:
- idonei accorgimenti per garantire la protezione dei dati dai rischi di: accesso abusivo ai dati, furto o smarrimento parziale o integrale dei supporti di memorizzazione, dei sistemi di elaborazione portatili e fissi (ad esempio, attraverso l'applicazione parziale o integrale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure informatiche di protezione che rendano inintelligibili i dati ai soggetti non legittimati);
- protocolli di comunicazione sicuri basati, ad esempio, sull'utilizzo di standard crittografici nella trasmissione elettronica dei dati;

- tecniche di etichettatura, nella conservazione e nella trasmissione di campioni biologici, mediante codici identificativi, oppure altre soluzioni che, considerato il numero di campioni utilizzati, li rendono non direttamente riconducibili agli interessati, permettendo di identificare questi ultimi solo in caso di necessità.

Con specifico riferimento alle operazioni di elaborazione dei dati della ricerca memorizzati su un database centralizzato, è necessario adottare, tra gli altri:

- idonei sistemi di autenticazione e di autorizzazione per il personale autorizzato in funzione dei compiti e delle esigenze di accesso e trattamento, avendo cura di utilizzare credenziali di validità limitata alla durata della ricerca e di disattivarle al termine della stessa;
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli autorizzati al trattamento;
- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Trasferimenti dei dati all'estero

Articolo 1, paragrafo 3 del Regolamento UE 2016/679: all'interno dell'Unione europea e dello spazio economico europeo (Islanda, Norvegia, Liechtenstein) non vi sono limiti legati alla protezione dei dati personali.

Occorre sempre valutare le modalità tecniche e assegnare il corretto livello di sicurezza (pseudonimizzazione, crittografia, tecniche di cifratura, …) in relazione alla tipologia dei dati: comuni o particolari (relativi alla salute, genetici, biometrici, giudiziari ...).

Articoli da 44 a 49 del Regolamento UE 2016/679: il trasferimento di dati personali verso Paesi non appartenenti all'Unione europea è in linea di principio vietato, se non sono presenti specifiche garanzie:

- adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;
- in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali tipo);
- in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (articolo 49 del Regolamento).

Il GDPR stabilisce l'obbligo per il Titolare del trattamento, ove questo sia effettuato da un'amministrazione pubblica, di designare un Responsabile della protezione dati. Il Responsabile protezione dati ha compiti di consulenza nei confronti del Titolare e dei soggetti designati o autorizzati al trattamento e di sorveglianza sull'osservanza del Regolamento.
Per dubbi o chiarimenti è possibile contattare il Responsabile per la protezione dei dati personali RPD/DPO scrivendo a: dpo@iusspavia.it

Per conoscere la normativa è possibile consultare:

Regolamento in materia di protezione dei dati personali in attuazione del Regolamento UE 2016-679.pdf

Definizioni:

Dato personale - qualsiasi informazione riguardante una persona fisica, identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Paesi Terzi extra UE– Paesi non appartenenti alla Spazio Economico Europeo (SEE, ossia UE + Norvegia, Liechtenstein, Islanda);

Referenti privacy – persone fisiche, nominate del Responsabile interno del trattamento (Direttore di Dipartimento, Dirigente), che hanno il compito di supporto il Responsabile in tutte le attività relative al trattamento dei dati personali, di interfacciarsi con il RPD per tutte le attività inerenti alla corretta gestione della tutela dei dati personali e per ogni comunicazione legata all'applicazione della normativa in materia;

Titolare del Trattamento - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali" (art. 4. par. 1 punto 7 del Regolamento (UE) 2016/679- RGPD)-IUSS nella persona del Magnifico Rettore;

Trattamento - qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.