UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Gestione dei progetti di ricerca scientifica e protezione dei dati personali

ai sensi del Regolamento UE 216/679 (GDPR)

Indice

Allegati:

Definizioni
Informativa dati particolari
Informatica dati personali
Scheda di analisi per progetto

Premessa

Scopo del documento è mettere a disposizione dei singoli ricercatori una guida pratica per una corretta gestione del trattamento dei dati personali nell'ambito delle attività di ricerca scientifica.

Un'efficace tutela dei dati personali nell'ambito della ricerca scientifica è conseguibile attraverso un approccio che analizzi le peculiarità di ogni singola attività di ricerca, non essendo possibile utilizzare soluzioni preconfezionate e generalizzate.

Le informazioni sensibili, quali ad esempio i dati relativi alla salute, meritano maggiore protezione, visto che il loro trattamento si associa a una maggiore probabilità di impatti negativi per gli interessati.

In caso di dubbi sul trattamento dei dati che si intende effettuare e per una corretta valutazione del rischio e delle misure di sicurezza da applicare è possibile contattare:

- **Team Privacy**: privacy@uniroma4.it
- **Responsabile della Protezione dei Dati**: dpo@uniroma4.it

1. DATI PERSONALI

Per dato personale si intende qualsiasi informazione che identifica o rende identificabile, direttamente o indirettamente, una persona fisica. L'espressione "qualsiasi informazione" va interpretata in maniera estensiva tale da ricomprendere informazioni sulle caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute, situazione economica, opinioni, ecc. di una persona fisica.

I dati personali comprendono:

- **dati personali (**art. 4 del GDPR cd. comuni)
  - es. nome e cognome, indirizzi di residenza, e-mail, numero di telefono, indirizzo IP

- **dati "particolari"** (art. 9 del GDPR)
  - origine razziale o etnica
  - opinioni politiche
  - convinzioni religiose o filosofiche
  - appartenenza sindacale
  - dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione
  - dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici
  - dati relativi alla salute: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute

- **dati giudiziari** (art.10 del GDPR). Si tratta di dati che possono rilevare:
  - l'esistenza di determinati provvedimenti giudiziari soggetti all'iscrizione del casellario giudiziale (es. provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione)
  - la qualità di imputato o di indagato.

Trattamento di dati personali

Il considerando 159 del GDPR prevede che "*il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE. Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica*".

Tutto ciò che si fa con i dati personali è considerata un'**operazione di trattamento**. A titolo di esempio, rientrano in tale nozione:

- la raccolta dei dati personali tramite la somministrazione di questionari
- la consultazione di un *database* contenente dati personali
- il raffronto di dati personali
- la comunicazione di dati personali ad un *partner* di progetto

- la cancellazione
- l'anonimizzazione
- la pseudonimizzazione

Occorre poi interrogarsi sulla necessità di utilizzare dati personali nell'ambito della ricerca o se invece quest'ultima può essere realizzata anche solo con dati anonimi. Tale ultima opzione è da preferire, a meno che l'utilizzo dei dati personali sia effettivamente necessario per raggiungere le finalità proprie della ricerca.

Tutela specifica dei dati particolari e dei dati giudiziari

All'art. 9, par. 1, del GDPR vige il divieto di trattare questa tipologia di dati.

Il trattamento di tali dati, per scopi statistici e scientifici, deve avvenire di regola in forma anonima (art. 7 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).

È prevista un'eccezione alla regola quando ricorrono le seguenti condizioni:

- l'interessato ha espresso liberamente il consenso sulle base degli elementi previsti per l'informativa (art. 7, art. 13 e 14 del GDPR);
- il consenso è manifestato per iscritto.

Pseudonimizzazione, anonimizzazione e dato anonimo

Nell'ambito della ricerca scientifica il ricercatore deve aver chiara la differenza tra l'utilizzo di un dato pseudonomizzato e un dato anonimo poiché solo rispetto a quest'ultima tipologia di dati non trovano applicazione le regole del GDPR.

La pseudonimizzazione è una elaborazione consistente nella sostituzione di un attributo di identificazione univoco legato ad una collezione di dati con uno pseudonimo, tale che il collegamento con l'interessato non sia più immediatamente possibile senza l'uso di informazioni aggiuntive, tenute separate e messe in sicurezza con misure tecniche ed organizzative adeguate.

L'anonimizzazione è invece il risultato di tecniche che vengono applicate ai dati personali al fine di rendere la re-identificazione ragionevolmente impossibile. Diversamente, la re-identificazione si verifica nel caso in cui, partendo da dati erroneamente ritenuti anonimi, si riesca a recuperare informazioni identificative degli interessati, sia direttamente, sia tramite metodi di correlazione e deduzione.

Pertanto, la pseudonimizzazione non consiste in una tecnica per mezzo della quale il dato diventa anonimo, ma si sostanzia in una misura di sicurezza. Il dato pseudonimizzato a differenza di quello anonimo rimane un dato personale e come tale deve essere trattato in conformità alla normativa sulla protezione dei dati.

In sintesi, nell'ambito di un'attività di ricerca possono essere trattati:

- **dati personali**
- **dati particolari**
- **dati anonimi** ai quali non si applica la normativa sulla protezione dei dati personali

2. PRINCIPI GENERALI DA OSSERVARE NEL TRATTAMENTO DEI DATI PERSONALI

Trasparenza e informazione agli interessati

Il principio di trasparenza implica che i dati siano trattati in maniera trasparente nei confronti dell'interessato e si concretizza negli obblighi informativi previsti agli artt. 13 e 14 del GDPR.

Il trattamento dei dati dovrà avvenire esclusivamente per le finalità indicate nell'informativa relativa allo specifico progetto di ricerca.

Quando la raccolta dei dati avviene presso l'Interessato, il Titolare del trattamento lo informa che i suoi dati sono trattati a fini scientifici ai sensi dell'art. 13 del GDPR.

Il ricercatore che tratta dati non ottenuti direttamente dall'interessato (ad esempio utilizza dati provenienti da cartelle cliniche) dovrà fornire le informazioni nelle modalità previste dall'art. 14 del GDPR. Nello specifico, il Titolare deve informare l'Interessato "*entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese in considerazione delle specifiche circostanze in cui i dati personali sono trattati*".

Casi in cui non vi è l'obbligo di informazione

Ai sensi dell'art. 4, par. 5, del GDPR, quando rendere l'informativa comporta uno sforzo sproporzionato rispetto al diritto tutelato, è possibile adottare idonee forme di pubblicità, quali:

- inserzione su un quotidiano di larga diffusione nazionale o annuncio presso un'emittente radiotelevisiva a diffusione nazionale (per trattamenti riguardanti soggetti distribuiti sull'intero territorio nazionale)

- inserzione in strumenti informativi in cui gli interessati sono normalmente destinatari (per specifiche categorie di soggetti identificate da particolari caratteristiche demografiche e/o particolari condizioni formative o occupazionali).

Il principio di liceità

Il principio di liceità è un principio disciplinato all'art. 5, lett. a), del GDPR e si sostanzia nella previsione di una serie di presupposti di liceità del trattamento, quali:

- consenso
- contratto
- obbligo legale
- salvaguardia di interessi vitali
- compito di interesse pubblico o connesso all'esercizio di pubblici poteri
- legittimo interesse del Titolare.

Si chiarisce la differenza tra il **consenso** ai sensi dell'art. 6 del GDPR e il **consenso informato** (e foglio illustrativo).

Consenso (artt. 6 e 9 del GDPR)	**Consenso informato e foglio illustrativo**
In linea generale il trattamento di dati personali per finalità di ricerca da parte di soggetti pubblici, tra cui quindi l'Università, non prevede l'obbligo di raccogliere il consenso, ad eccezione di quanto previsto per il trattamento di dati personali di cui all'art. 9 del GDPR idonei a rivelare lo stato di salute per scopi di ricerca scientifica in campo medico, biomedico o epidemiologico in cui è invece necessario acquisire il consenso (ex art. 110 Codice Privacy, art. 11 Codice deontologico). Per essere **valido** il consenso deve essere: • preceduto dall'aver reso l'informativa sul trattamento dei dati personali (art. 13 del GDPR); • espresso liberamente, in modo inequivocabile e non condizionato, ad esempio, alla prestazione di un servizio; • specifico in relazione a ciascuna finalità del trattamento; • presentato in maniera distinta da altre richieste, in forma comprensibile e utilizzando un linguaggio semplice e chiaro • esplicito ovvero manifestato per iscritto. Il consenso può essere revocato nella stessa maniera in cui è stato prestato. Quando la raccolta di dati particolari è effettuata con modalità – quali interviste telefoniche o assistite da elaboratore o simili – che rendono particolarmente gravoso acquisirlo per iscritto, il consenso, purché esplicito, può essere documentato per iscritto. In tal caso, la documentazione dell'informativa resa all'interessato e dell'acquisizione del relativo consenso è conservata dal titolare del trattamento per tre anni.	Il **consenso informato** è inteso come l'espressione volontaria e libera di un soggetto di partecipare alla ricerca. Tale consenso può essere raccolto solo dopo aver comunicato ai partecipanti le informazioni contenute nel foglio informativo e verificato che gli stessi le abbiano pienamente comprese. Tale consenso deve essere di regola scritto, datato e firmato dai partecipanti o, nel caso di minori o soggetti incapaci, dai loro rappresentanti legali. Il consenso informato alla ricerca può essere reso anche in modo implicito, tramite comportamenti concludenti. Il **Foglio Illustrativo** sul progetto di ricerca: si tratta di un documento nel quale si spiega ai potenziali partecipanti di cosa tratta la ricerca, gli scopi che la stessa si prefigge, che cosa comporta la loro eventuale partecipazione nonché gli eventuali rischi. Deve essere utilizzato un linguaggio semplice e chiaro in modo che i partecipanti siano messi in grado di decidere consapevolmente e senza alcuna pressione se partecipare o meno alla stessa; deve inoltre essere evidenziato ai partecipanti che la loro mancata partecipazione non produrrà alcun effetto negativo o pregiudizievole nei loro confronti. Copia del foglio informativo viene consegnata al partecipante.
In sintesi	
Il consenso disciplinato dal GDPR attiene invece esclusivamente al trattamento dei dati personali e deve essere raccolto nel solo caso in cui vi sia la necessità di trattare, per le finalità della ricerca, dati particolari (relativi alla salute, genetici, biometrici, origine razziale o etnica, convinzioni religiose…), dati relativi a reati e condanne penali oppure nell'ambito della ricerca medica, biomedica ed epidemiologica.	Il consenso informato è uno standard etico e deve essere sempre raccolto da tutti i partecipanti per ogni progetto di ricerca.

Limitazione delle finalità

Di norma, ai sensi dell'art. 5, par. 1, lett. b), del GDPR, i dati sono "*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità*". Tuttavia, la "presunzione di compatibilità" di cui all'articolo citato stabilisce che "*un ulteriore trattamento [...] per finalità [...] di ricerca scientifica [...] non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali*".

Minimizzazione dei dati

Per il principio di minimizzazione di cui all'art. 5 del GDPR i dati personali devono essere:

- adeguati
- pertinenti
- limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Nell'ambito della ricerca scientifica, è possibile rispettare il principio di minimizzazione prevedendo l'obbligo di specificare i quesiti di ricerca e di valutare la tipologia e la quantità di informazioni necessarie per rispondere adeguatamente a tali quesiti.

La definizione dei dati necessari dipenderà sempre dalle finalità della ricerca, anche quando quest'ultima ha natura esplorativa, e avverrà comunque nel rispetto del principio della limitazione delle finalità a norma dell'art. 5, par. 1, lettera b), del GDPR.

Si rileva che i dati devono essere resi anonimi quando è possibile effettuare una ricerca scientifica con dati anonimizzati.

Principio di conservazione

Devono essere fissati periodi di conservazione dei dati proporzionati alle finalità. Come previsto dall'art. 5, par. 1, lett. e), del GDPR, "*i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse [...] di ricerca scientifica [...] conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato*".

Nel definire i periodi di conservazione devono essere tenuti in considerazione criteri quali la durata e lo scopo della ricerca. Inoltre, occorre osservare quali disposizioni nazionali possono disciplinare il periodo di conservazione.

Integrità e riservatezza

Il principio di integrità e riservatezza deve essere letto in combinato disposto con i requisiti di cui all'art. 32, par. 1 e all'art. 89, par. 1, del GDPR (Sicurezza del trattamento). Le disposizioni citate devono essere rispettate integralmente. Pertanto, tenuto conto dei rischi elevati di cui sopra, occorre implementare misure tecniche e organizzative adeguate a garantire un livello sufficiente di sicurezza.

Esempi di misure di sicurezza:

- pseudonimizzazione
- cifratura.

Si vedano anche le Linee-guida 4/2019 del Comitato (13.11.2019) sulla protezione dei dati fin dalla progettazione e per impostazione predefinita: https://edpb.europa.eu/our-work-tools/public-consultations- art-704/2019/guidelines-42019-article-25-data-protection-design_en.

È importante osservare che i dati personali (ad esempio relativi alla salute) pseudonimizzati sono considerati ancora dati personali ai sensi dell'art. 4, par. 1, del GDPR e non devono essere confusi con i dati anonimizzati, che invece non consentono alcun collegamento con singoli Interessati.

3. SOGGETTI NELL'AMBITO DELL'ATTIVITA' DI RICERCA

L'interessato

L' interessato è la persona fisica cui i dati personali si riferiscono e che sono oggetto di trattamento. Nell'ambito della ricerca liInteressato è, ad esempio, chi è chiamato a compilare un questionario, la persona che si sottopone volontariamente ad un esperimento o alla quale appartiene il campione biologico prelevato.

Il Titolare del trattamento dei dati

Il Titolare del trattamento è la persona fisica o giuridica che determina le finalità ed i mezzi del trattamento.

Per le attività di ricerca svolte nell'ambito dell'Università, il Titolare è l'Università degli Studi di Roma "Foro Italico" (in seguito Titolare), rappresentata legalmente dal Rettore.

Il Responsabile della Protezione dei dati personali (in seguito DPO)
È un soggetto designato in funzione delle qualità professionali, in particolare delle conoscenze specialistiche della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del GDPR. In particolare:

- informa e fornisce consulenza al Titolare e ai dipendenti
- sorveglia l'osservanza del GDPR nonché delle politiche del titolare
- fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati
- coopera con l'Autorità di controllo
- funge da punto di contatto per l'Autorità di controllo

Il Coordinatore del Progetto o Responsabile scientifico (in seguito PI)
Il PI è individuato come soggetto Designato nella gestione del trattamento dei dati personali ed ha l'obbligo di attenersi a quanto previsto dalla normativa sul trattamento dei dati personali e alle istruzioni impartite dal Titolare. In particolare, il PI è tenuto a:

- adottare opportune misure di sicurezza per garantire la protezione dei dati personali trattati
- garantire che al momento della raccolta dei dati, sia resa all'interessato la dovuta informativa, ai sensi degli artt. 13 e 14 del GDPR
- compilare, prima dell'avvio di ogni progetto di ricerca, la "Scheda di analisi per progetti di ricerca", proposta dal CODAU, ed inviarla al Team privacy (privacy@uniroma4.it), unitamente all'informativa
- collaborare per la corretta gestione delle richieste di esercizio dei diritti degli interessati
- segnalare con tempestività al DPO eventuali anomalie, incidenti, furti, perdite di dati o altre eventuali violazioni di dati personali (data breach)
- vigilare sul rispetto delle disposizioni di legge in materia di protezione dei dati personali, da parte del team di ricerca

Team di ricerca
All'interno del team di ricerca, il PI deve individuare uno o più soggetti autorizzati al trattamento dei dati personali. Tali soggetti vengono allo scopo designati "Autorizzati al trattamento" tramite la sottoscrizione della Scheda di analisi per progetti di ricerca. Spetterà solo ai ricercatori "autorizzati", e non agli altri membri del team, procedere al trattamento dei dati personali e dare applicazione alle relative misure di sicurezza.

Partner di un progetto di ricerca congiunto
In relazione al tipo di trattamento da effettuare, ciascun partner può alternativamente assumere i seguenti ruoli:

- contitolare del trattamento, quando determina congiuntamente all'altro partner le finalità e i mezzi del trattamento. In tal caso, dovrà essere sottoscritto un accordo interno di contitolarità dei dati tra i due o più partner come previsto dall'art. 26 del GDPR
- titolare autonomo, quando ciascun partner effettua autonomamente il trattamento, sebbene i trattamenti siano connessi
- responsabile del trattamento, quando un partner effettua il trattamento dei dati per conto dell'altro. In tal caso, dovrà essere sottoscritto un apposito contratto o altro atto giuridico di nomina a Responsabile del trattamento come previsto dall'art. 28 del GDPR.

4. OBBLIGHI NELL'AMBITO DELLA RICERCA SCIENTIFICA

Obblighi in fase di progettazione

L'attività di ricerca deve essere preceduta dalla redazione di un progetto, in conformità agli standard metodologici del pertinente settore disciplinare, anche al fine di documentare che il trattamento dei dati personali avvenga per effettivi scopi statistici e/o scientifici.

In particolare, è necessario:

- preliminarmente compilare la scheda di analisi per progetti di ricerca anche ai fini dell'analisi dei rischi
- verificare che i dati personali che si prevede di trattare nell'ambito del progetto di ricerca siano necessari, pertinenti e indispensabili per raggiungere le finalità della ricerca

- effettuare l'analisi dei rischi collegati al trattamento di dati personali per individuare le misure di sicurezza adeguate a proteggere i dati dal rischio di distruzione, perdita di disponibilità e/o di riservatezza ai sensi dell'art.35 GDPR. Pertanto, verificare se, in ragione della natura, dell'oggetto e delle finalità della ricerca e nel caso di utilizzo di nuove tecnologie (App, social network, ecc.) vi sia un rischio elevato per i diritti e le libertà degli interessati. È possibile utilizzare il *tool* messo a disposizione dal Garante della privacy francese:https://www.garanteprivacy.it/web/guest/home/docweb//docweb display/docweb/8581268
- individuare all'interno del team di ricerca, i soggetti autorizzati al trattamento dei dati personali e istruirli adeguatamente in materia
- qualora nelle attività di ricerca ci si avvalga di un soggetto esterno per la fornitura di un servizio che implica il trattamento di dati personali (es. il gestore di una piattaforma), è comunicarlo al Team Privacy al fine della nomina di "Responsabile del trattamento" ai sensi dell'art. 28 GDPR
- redigere e fornire ai partecipanti alla ricerca, l'informativa sul trattamento dei dati personali (artt. 13 e 14 GDPR) e raccogliere l'eventuale consenso al trattamento dei dati nei casi in cui sia necessario (consenso per la ricerca medica, biomedica e epidemiologica; consenso per il trattamento dei dati particolari e dei dati giudiziari)

Approfondimento: "Valutazione d'impatto sulla protezione dei dati" (di seguito DPIA) per lo specifico progetto di ricerca (ex artt. 35-36 GDPR)
Non tutti i progetti di ricerca comportano la necessità di effettuare una valutazione di impatto. In alcuni casi, la necessità di effettuare la valutazione di impatto dipende da una valutazione delle caratteristiche del trattamento e dalla sua idoneità a rappresentare rischi elevati. In altri casi, la necessità di effettuare una valutazione di impatto su progetti di ricerca è un requisito richiesto dalla legge. Casi in cui la valutazione di impatto sulla protezione dei dati è obbligatoria per legge: a) Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento; b) Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento; c) Trattamenti non occasionali di dati relativi a soggetti vulnerabili (es. minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo); d) Trattamenti che comportano lo scambio tra diversi Titolari di dati su larga scala con modalità telematiche. La DPIA deve essere effettuata prima di procedere al trattamento e dovrà essere conservata allegata alla Scheda di progetto. 2 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/905935 La DPIA deve essere effettuata tenuto conto del parere del Responsabile per la Protezione dei Dati.

Obblighi durante lo svolgimento dell'attività di ricerca

Durante lo svolgimento dell'attività di ricerca, è necessario:

- applicare le misure di sicurezza individuate eventualmente con l'analisi dei rischi (quali la *pseudonimizzazione*, la cifratura per i dati, i backup periodici, gli accessi limitati, i profili di autenticazione e di autorizzazione)
- vigilare sull'applicazione e osservanza della normativa sulla protezione dei dati da parte dei ricercatori autorizzati al trattamento dei dati e degli eventuali Responsabili al trattamento (es. fornitori di un servizio;
- collaborare per la corretta gestione delle richieste di esercizio dei diritti degli interessati (http://www.uniroma4.it/?q=taxonomy/term/263)
- segnalare tempestivamente al Titolare eventuali violazioni di dati personali (DATA BREACH) intervenute nell'ambito della ricerca.

Obblighi al termine dell'attività di ricerca

A conclusione dell'attività di ricerca, è necessario:

- cancellare i dati personali trattati o renderli completamente anonimi con specifiche tecniche di anonimizzazione
- depositare l'integrale documentazione privacy presso il Team Privacy (progetto, informativa, consensi, scheda analisi progetto etc.) che ne curerà la conservazione in forma riservata per cinque anni dalla conclusione programmata della ricerca.

5. COMUNICAZIONE DI DATI PERSONALI AD ALTRI PARTNER DI RICERCA NELL'AMBITO DI RICERCHE CONGIUNTE

Nell'ambito dell'attività di ricerca congiunta con altri partner di ricerca (università, enti di ricerca ecc..) è sempre da preferire che la comunicazione di dati avvenga in forma anonima.

Se tuttavia, per il raggiungimento delle finalità della ricerca è necessario comunicare i dati personali ad un altro Partner di progetto, ciò è possibile esclusivamente nel rispetto delle seguenti condizioni:

- sia stato sottoscritto uno specifico accordo tra i partner che specifichi il ruolo privacy rivestito da ciascun partner in relazione ai trattamenti effettuati nell'ambito dell'attività di ricerca
- la sussistenza della "necessità" di comunicazione dei dati tra Partner per le finalità della ricerca e che tale necessità emerga dalla descrizione delle attività di progetto
- l'individuazione di adeguate misure tecniche ed organizzative nella trasmissione dei dati, quali, ad esempio, la pseudonimizzazione, la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento ecc.

Le disposizioni si applicano anche alla comunicazione di dati personali a Università o istituti o enti di ricerca o ricercatori residenti in un Paese appartenente all'Unione europea o il cui ordinamento assicuri comunque un livello di tutela delle persone adeguato.
Per **comunicazioni a Paesi extra UE**, il trasferimento dei dati è consentito solo nei confronti dei Paesi per i quali sussiste una decisione di adeguatezza della Commissione o offrono garanzie appropriate o opportune (artt. 46-49 GDPR).

6. DIFFUSIONE DI DATI PERSONALI

E' consentito diffondere i dati personali, anche con pubblicazioni, soltanto in forma aggregata o con modalità che non rendano identificabili gli interessati, salvo che la diffusione riguardi variabili pubbliche.

7. DISPOSIZIONI PARTICOLARI PER LA RICERCA MEDICA, BIOMEDICA EDEPIDEMIOLOGICA

Normativa sulla ricerca medica, biomedica ed epidemiologica

La ricerca medica, biomedica ed epidemiologica è sottoposta all'applicazione delle 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, conformemente agli standard metodologici del pertinente settore disciplinare (Pubblicate sulla Gazzetta Ufficiale n. 11 del 14 gennaio 2019).
Si svolge nel rispetto degli orientamenti e delle disposizioni internazionali e comunitarie in materia, quali la Convenzione sui diritti dell'uomo e sulla biomedicina del 4 aprile 1997, ratificata con legge 28 marzo 2001, n. 145, la Raccomandazione del Consiglio d'Europa (97)8 adottata il 13 febbraio 1997 relativa alla protezione dei dati sanitarie la dichiarazione di Helsinki dell'Associazione medica mondiale sui principi per la ricerca che coinvolge soggetti umani.
Le informazioni sul trattamento di dati personali contenute nel progetto di ricerca devono mettere in grado gli interessati di distinguere le attività di ricerca da quelle di tutela della salute.
In caso di consenso ad una indagine medica o epidemiologica, all'interessato è richiesto di dichiarare se vuole conoscere eventuali scoperte inattese che emergono a suo carico durante la ricerca, ai sensi dell'art. 8 delle 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.

Raccolta dei dati

È necessario prestare specifica attenzione nella selezione del personale preposto alla raccolta dei dati personali e delle modalità di rilevazione, in modo da garantire il rispetto delle Regole deontologiche e la tutela dei diritti degli interessati.
Il personale preposto alla raccolta di dati personali, oltre a seguire le istruzioni ricevute deve:

- rendere nota la propria identità e funzione, nonché le finalità della raccolta, anche attraverso adeguata documentazione
- fornire le informazioni di cui all'art. 13 del GDPR
- seguire le indicazioni relative al consenso
- non svolgere contestualmente, presso gli stessi interessati, attività di rilevazione di dati personali per conto di più titolari, salvo espressa autorizzazione
- provvedere tempestivamente alla correzione degli errori e delle inesattezze delle informazioni acquisite nel corso della raccolta
- assicurare una particolare diligenza nella raccolta delle particolari categorie di dati (art. 9 GDPR).

Dati genetici/Campioni biologici

Il trattamento di campioni biologici prelevati per finalità di ricerca scientifica e statistica è consentito solo se volto alla tutela della salute:

- dell'interessato
- di terzi

- della collettività in campo medico, biomedico ed epidemiologico.

Il trattamento deve essere svolto sulla base di un progetto redatto conformemente agli standard del pertinente settore disciplinare, anche al fine di documentare che il trattamento dei dati e l'utilizzo dei campioni biologici sia effettuato per idonei ed effettivi scopi scientifici

Il Progetto di Ricerca

Il Progetto di ricerca deve specificare le misure da adottare per garantire il rispetto delle Prescrizioni contenute nelle autorizzazioni generali e che risultano compatibili con il Regolamento e con il D.lgs. n. 101/2018 – 13 dicembre 2018, e della normativa sulla protezione dei dati personali:

- individua gli eventuali responsabili del trattamento (art. 28 del GDPR);
- indica l'origine, la natura e le modalità di prelievo e conservazione dei campioni, e le misure adottate per garantire la volontarietà del conferimento del materiale biologico da parte dell'interessato.

Conservazione del progetto

La conservazione del Progetto è a cura del PI in forma riservata per cinque anni dopo la conclusione della ricerca.
Quando le finalità della ricerca possono essere realizzate soltanto tramite l'identificazione, anche solo temporanea, degli interessati, il PI adotta specifiche misure per mantenere separati i dati identificativi dai campioni biologici, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego dimezzi manifestamente spropositati.

Consenso

È necessario acquisire il consenso al trattamento dei dati genetici per fini di ricerca e all'interessato è richiesto di dichiarare se vuole conoscere o meno i risultati della ricerca.
Quando non è possibile acquisire il consenso degli interessati, il titolare del trattamento deve documentare, nel progetto di ricerca, la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali 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.
Il consenso non è necessario quando la ricerca è effettuata in base a disposizione di legge o di regolamento al diritto europeo.
Nel caso in cui l'interessato revochi il consenso al trattamento il campione biologico è distrutto salvo che il campione non possa più essere riferito ad una persona identificata o identificabile.

Comunicazione e diffusione dei dati

Si seguono le norme generali che disciplinano la comunicazione e la diffusione delle particolari categorie di dati.

Modalità di trattamento

Nel trattamento successivo alla raccolta retrospettiva dei dati, sono adottate tecniche di cifratura o di pseudonimizzazione oppure altre soluzioni che, considerato il volume dei dati trattati, la natura, l'oggetto, il contesto e le finalità del trattamento li rendono non direttamente riconducibili agli interessati, permettendo di identificare questi ultimi solo in caso di necessità. In questi casi, i codici utilizzati non sono desumibili dai dati personali identificativi degli interessati, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato e sia motivato, altresì, per iscritto, nel progetto di ricerca.

Conservazione dei dati e dei campioni

I dati e i campioni biologici utilizzati per l'esecuzione della ricerca sono conservati mediante tecniche di cifratura o l'utilizzazione di codici identificativi oppure di altre soluzioni che, considerato il numero dei dati e dei campioni conservati, non li rendono direttamente riconducibili agli interessati, per un periodo di tempo non superiore a quello necessario agli scopi peri quali essi sono stati raccolti o successivamente trattati.
A tal fine, è indicato nel progetto di ricerca il periodo di conservazione, successivo alla conclusione dello studio, al termine del quale i predetti dati e campioni sono anonimizzati.

8. ATTIVITA' DI RICERCA NELL'AMBITO DI PROGETTI EUROPEI

Raccomandazioni per il coordinatore del Progetto e dei Partner

Nella fase di definizione il Partner e anche gli altri Partner devono avere cura di definire i ruoli nell'ambito della Protezione dei dati personali (Titolarità autonoma, Contitolarità del trattamento e Responsabilità del trattamento dei dati personali) regolamentando tali aspetti ad esempio nel *Consortium agreement.*
Lo scopo di definizione dei ruoli risponde all'esigenza di individuare i Titolari del Trattamento al fine di fornire le informative agli interessati ai sensi 13 e 14 GDPR.
Inoltre, si raccomanda la preliminare e tempestiva definizione anche in vista della connessa documentazione:

- Data Sharing Agreement (DSA): accordo finalizzato a stabilire lo scopo della condivisione dei dati e nella condivisione a chiarire i loro ruoli e responsabilità
- Joint Controllership agreement (JCA): accordo che determina i diritti e gli obblighi dei titolari del trattamento per il trattamento congiunto dei dati personali ai sensi dell'art. 26 GDPR.

Nel caso in cui uno o più Partner non è appartenente all'Unione Europea e non rientra nell'ipotesi dell'articolo 45 GDPR è opportuno predisporre il seguente documento:

- Data Trasfer Agreement (DTA): accordo nel quale vengono incluse e sottoscritte le clausole di contratto standard. Tali clausole, essendo state predisposte direttamente dalla Commissione Europea, garantiscono in ogni caso l'adeguatezza della tutela dei dati personali da parte dell'azienda del Paese terzo che li riceve.

Per tutto quanto non espressamente disciplinato dal presente articolo si invita a seguire quanto previsto al capitolo 4 "Obblighi nell'ambito della ricerca scientifica" e in generale quanto previsto nel presente documento avendo cura di coinvolgere, fin dalla fase di avvio, il DPO dell'Università Foro Italico e il Team Privacy (Premessa*-).

9. MISURE DI SICUREZZA

Il Responsabile del progetto dovrà individuare, per ogni singola ricerca, le misure adeguate per garantire la protezione dei dati, tenendo conto della natura, oggetto e contesto e finalità del trattamento, nonché dei costi di attuazione, ai sensi dell'art. 32 del GDPR.
Si riportano di seguito alcune indicazioni di massima da adottare affinché il trattamento dei dati personali utilizzati per attività di ricerca sia effettuato in conformità con quanto previsto dal GDPR e dalla Circolare AGID n. 2/2017:

- la pseudonimizzazione
- l'anonimizzazione
- la cifratura dei dati personali
- la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- cifratura per i dispositivi portatili
- installazione di firewall e antivirus locali.

Trattamento cartaceo

Conservare per tutta la durata del progetto di ricerca la documentazione cartacea contenente i dati personali in archivi ad accesso controllato in modo da escludere l'accesso da parte di persone non autorizzate (ad esempio utilizzando armadi muniti di serratura):

- non lasciare la documentazione cartacea contenente dati personali incustodita sulla scrivania e riporla negli appositi archivi al termine del suo utilizzo
- qualora la documentazione cartacea debba essere trasmessa ad altri uffici dell'Università, adottare idonee misure per salvaguardare la riservatezza dei dati personali (es. in busta chiusa)
- al termine della conclusione del progetto di ricerca, riporre tutta la documentazione di progetto in scatoloni chiusi da consegnare al Team Privacy che li conserverà in luoghi ad accesso controllato
- sull'etichetta degli scatoloni specificare i seguenti dati in modo da permettere una corretta gestione:
  - titolo del progetto
  - durata del progetto (dal… al….)
  - nome del responsabile del Progetto
  - data a partire dalla quale si possono distruggere
  - qualora sia necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti"

Trattamento elettronico

Individuare sulla base dell'analisi della categoria dei dati personali trattati ovvero se dati comuni o particolari (relativi alla salute, genetici, biometrici, giudiziari etc.) il corretto livello di sicurezza da applicare al trattamento (pseudonimizzazione, crittografia, tecniche di cifratura etc.):

- valutare il tipo di supporto/dispositivo su cui salvare i dati personali trattati e che siano attive politiche adeguate di backup dei dati sia nel caso in cui gli stessi vengano memorizzati su sistemi di storage
- assicurarsi che i dati personali non vengano salvati dai collaboratori su unità di memoria esterne (hard disk, pendrive, DVD) a meno che non siano dotati di appositi sistemi di crittografia (in modo da proteggere i dati anche nel caso in cui tali unità di memoria vengano smarrite o rubate)
- verificare la completa cancellazione dei dati in caso di dismissione/riparazione/riutilizzo di hardware contenente i dati stessi.

Autenticazione e Autorizzazione

Individuare i soggetti autorizzati a trattare i dati personali e definire le corrette autorizzazioni di accesso ai dispositivi e alle aree ove i dati sono trattati e/o conservati; qualora non sussistano più le ragioni per l'accesso ai dati (ad es. uscita di un ricercatore dal team di ricerca, conclusione del progetto di ricerca) procedere a far rimuovere le relative autorizzazioni.

Adottare meccanismi di autenticazione (pin, password etc.) per l'accesso al dato e/o ai sistemi che trattano il dato, attivando, dove possibile, meccanismi di crittografia dei supporti fisici per tutti i sistemi (in particolare quelli mobili quali laptop e cellulari).

Disposizioni Organizzative

Istruire adeguatamente i collaboratori del team di ricerca che effettuano il trattamento di dati personali sulle corrette modalità da seguire e le misure di sicurezza da adottare.

Postazioni di Lavoro

Prestare attenzione alla postazione da cui si effettua il trattamento dei dati. Le postazioni private (pc fissi, tablet, laptop, cellulari), ad esempio, potrebbero non essere dotate di tutti i meccanismi di difesa adeguati (antivirus, firewall) e se collegati alla rete internet, essere maggiormente soggetti ai rischi di virus, malware, ransomware.

Utilizzo di sistemi di elaborazione

Nel caso di utilizzo, anche a titolo gratuito, di sistemi di elaborazione dati non appartenenti all'Università degli Studi di Roma "Foro Italico", valutare preventivamente tali sistemi e, in particolare, procedere a richiedere al fornitore una dichiarazione attestante la conformità al Regolamento EU 2016/676 (GDPR) e l'adozione di misure di sicurezza adeguate al trattamento dei dati da effettuare.