Linee Guida GDPR (Regolamento UE n. 679/2016)

Premessa

Obiettivo di questa pagina è fornire le informazioni necessarie alla corretta gestione dei dati personali raccolti direttamente o indirettamente nell'ambito dell'attività di ricerca.

Per adempiere a quanto prescritto dalla normativa europea e nazionale in materia, l'attività di ricerca che preveda il trattamento di dati personali dovrà essere preceduta dalla redazione di atti utili a documentare il trattamento di tali dati per effettivi scopi statistici e/o scientifici.

Il trattamento dei dati personali dovrà essere improntato al rispetto dei principi di liceità, correttezza, trasparenza, pertinenza, non eccedenza ed in modo da garantire un'adeguata sicurezza dei dati personali.

Qualora l'attività di ricerca comporti, oltre al trattamento di dati personali dei partecipanti, anche un rischio per il benessere psico-fisico degli stessi, dovrà essere richiesto il preventivo parere del Comitato etico per i rispettivi casi di competenza, che prevede una valutazione integrata anche degli aspetti relativi alla protezione dei dati personali.

Definizioni utili

"**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 (art. 4, n. 2 GDPR);

"**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 (art. 4, n. 1 GDPR);

"**categorie particolari di dati personali (dati sensibili)**": i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, par. 1, GDPR);

"**dati genetici**": i 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 (art. 4, n. 13 GDPR);

"**dati biometrici**": i 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 (art. 4, n. 14 GDPR);

"**dati relativi alla salute**": i 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 (art. 4, n. 15 GDPR);

"**dato giudiziari**": i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 GDPR)

"**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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, n. 7 GDPR);

"**responsabile del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, n. 8 GDPR);

"**responsabile della protezione dei dati**": professionista esperto nella protezione dei dati i cui compiti sono valutare ed organizzare la gestione del trattamento dei dati personali all'interno di ciascuna organizzazione (artt. 37, 38 e 39 GDPR);

"**autorizzato**": chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento (art. 29 GDPR)

"**comunicazione**": il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione (art. 2-ter, co. 4, lett. a) del Codice privacy);

"**diffusione**": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 2-ter, co. 4, lett. b) del Codice privacy):

"**informazioni anonime**": le informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato (Considerando 26 del GDPR).

Prescrizioni generali per chi svolge attività di ricerca

Il CNR è "titolare del trattamento" dei dati personali effettuato nell'ambito dell'esecuzione dei propri compiti istituzionali, tra cui l'attività di ricerca scientifica.

Il Direttore di Istituto è Responsabile interno del trattamento, ovvero il braccio operativo del titolare e punto di contatto per l'esercizio dei diritti dell'Interessato.

Il Referente privacy è il punto di contatto con il responsabile della protezione dei dati e con la Direzione Generale per l'applicazione delle disposizioni in materia di protezione dei dati personali e supporto alle attività di gestione degli adempimenti connessi alla protezione dei dati.

Il Responsabile dell'attività d ricerca assume il ruolo di "Autorizzato al trattamento".

Fermo restando quanto stabilito dalle normative vigenti (in particolare, GDPR, Codice privacy, Regole deontologiche) queste figure sono tenute all'osservanza, delle seguenti prescrizioni generali:

- il trattamento dei dati dovrà avvenire esclusivamente per le finalità indicate nell'informativa (ex art. 13 e 14 GDPR) relativa alla specifica attività di ricerca;
- il trattamento dei dati personali dovrà avvenire nel rispetto dei principi di liceità, correttezza, trasparenza, adeguatezza, pertinenza, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione;
- l'accesso ad eventuali banche dati dedicate all'attività di ricerca dovrà essere specificatamente autorizzato dal responsabile dell'attività di ricerca;
- l'applicazione delle misure tecniche ed organizzative indicate dal titolare del trattamento (ai sensi dell'art. 32 GDPR);
- nei casi necessari, lo svolgimento di una "valutazione d'impatto sulla protezione dei dati" per la specifica attività di ricerca (ai sensi dell'artt. 35-36 GDPR);
- la comunicazione immediata al Titolare (Direttore) di casi di violazione di dati personali avvenuti nell'ambito della stessa attività di ricerca (art. 34 GDPR).

Nel portale INO "Area Riservata" è presente la sezione "GDPR" nella quale è possibile reperire la seguente documentazione:

1. Norme di Comportamento:

Circolare interna attività di ricerca
Circolare interna attività gestionale amministrativa
Guida all'applicazione del Regolamento europeo
Linee Guida sulla Valutazione d'impatto (DPIA)
Linee guida per effettuare la valutazione d'impatto sulla protezione dei dati, come richiesto dall'art. 35 comma 1 del GDPR (General data Protection Regulation EU 2016/679)
Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679:

- Modello interno per la raccolta delle informazioni sulla violazione
- Modello notifica al Garante
- Modello di comunicazione della violazione all'interessato
- Registro delle violazioni dei dati

2. Modulistica

(Informativa, accordo di contitolarità, consenso informato per eventi ecc.). I moduli sono diversificati da un numero corrispondente all'allegato di riferimento.

3. Provvedimenti CNR

Direttiva - Notifica di violazione dei dati personali ex art.33 Regolamento
Provv. n. 27 - Compiti e funzioni dei Responsabili interni CNR in materia di Trattamento dei dati personali
Provv. n. 46 - Nomina del Responsabile della Protezione dei Dati personali (RDP)

4. Principali Provvedimenti del Garante

Provvedimento Garante - Amministratore di Sistema
Provvedimento Garante - Posta Elettronica e Internet
Provvedimento Privacy - Data Breach
Provvedimento Garante - Cloud Computing
Provvedimento Garante – Videosorveglianza
Provvedimento Garante - Smaltimento delle Apparecchiature Elettroniche
Provvedimento Garante - Rfid

Obblighi del Responsabile dell'attività di ricerca

Se non si trattano dati personali il Responsabile scientifico dell'attività di ricerca deve sottoscrivere la Liberatoria (*Modulistica → All. 3B*)

Se si trattano dati personali, prima dell'inizio dell'attività di ricerca, il Responsabile scientifico della ricerca è tenuto all'espletamento di alcuni adempimenti atti a documentare che il trattamento dei dati avvenga per effettivi scopi statistici e/o scientifici:

- Redazione dell'informativa ex art. 13 GDPR (se i dati non sono raccolti direttamente presso l'interessato, ex art. 14 GDPR) e, quando necessario, del consenso al trattamento delle categorie particolari di dati personali, dei dati giudiziari e nell'ambito della ricerca medica, biomedica ed epidemiologica (*Modulistica → 2) Informative → All. 3/3A e all. 4/4A*);
- Redazione del Documento di supporto al Registro del trattamento dati compilato in conformità agli standard metodologici del pertinente settore disciplinare, atto a documentare che il trattamento sia effettuato per idonei ed effettivi scopi statistici e scientifici, ivi specificati (*Modulistica → All. 3A*);
- Redazione del documento di Valutazione d'impatto (se necessaria) (DPIA) (*Modulistica → All. 5*)[1];
- Sottoscrizione della Dichiarazione impegno alla riservatezza per tutto il personale coinvolto nell'attività di ricerca, compreso lo stesso Responsabile scientifico (*Modulistica → All. 1*);
- Predisposizione Decreto di autorizzazione al trattamento dati personali (*Modulistica → All. 10 e All. 10A*).

La suddetta documentazione deve essere inviata al Referente Privacy dell'Istituto Nazionale di Ottica all'indirizzo privacy.gdpr@ino.cnr.it, la prima volta e ogni qualvolta debba essere aggiornata.

Comunicazione dei dati 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 ricerca, ciò è possibile esclusivamente nel rispetto delle seguenti condizioni:

- 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 ricerca;
- l'individuazione del ruolo privacy rivestito da ciascun Partner in relazione ai trattamenti effettuati nell'ambito della ricerca. Quando sia ravvisabile una situazione di contitolarità, andrà sottoscritto, a seconda dei casi, un accordo interno di Contitolarità (art. 26 GDPR) in cui andranno stabiliti i rispettivi

[1] Ci sono varie metodologie e standard di riferimento:
- Software CNIL (Autorità Garante Francese): https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/858
- Software ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione): https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9254237

ruoli e responsabilità o una nomina a Responsabile del trattamento (art. 28 GDPR) (*Modulistica → All. 6/6A; All. 7/7A; All. 8*);
- l'individuazione e la documentazione 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.

Diffusione dei dati

È consentito diffondere, anche mediante pubblicazione, i risultati della ricerca soltanto in forma aggregata ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti, salvo che la diffusione riguardi variabili pubbliche.

Trattamento di dati particolari per scopi di ricerca medica, biomedica ed epidemiologica

I protocolli per la ricerca scientifica in campo medico, biomedico ed epidemiologico vanno sottoposti alla preventiva approvazione del comitato etico territorialmente competente.

Le misure di sicurezza nel trattamento dei dati personali

Ai sensi dell'art. 32, par. 1 del Regolamento EU 2016/676 (GDPR) per ogni trattamento di dati personali il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza appropriato rispetto al rischio.

L'attività di ricerca che comporta il trattamento di dati personali (quali ad es. la raccolta di dati dei volontari), è soggetta all'applicazione della normativa sulla protezione dei dati. Il ricercatore dovrà pertanto individuare, in relazione ad ogni singola attività di ricerca, le misure adeguate che garantiscano la protezione dei dati trattati, avendo riguardo allo stato dell'arte, ai costi di attuazione, a natura, oggetto, contesto e finalità del trattamento.

Il Regolamento EU indica a titolo esemplificativo già alcune misure: 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; analogamente la Circolare AGID n. 2 del 18/04/2017 sulle Misure Minime di Sicurezza suggerisce alcune prescrizioni da adottare nel trattamento dei dati personali in base al livello di rischio individuato per ogni singolo trattamento, quali ad es. la cifratura per i dispositivi portatili, l'installazione di firewall e antivirus locali, ecc.

Si precisa che la modulistica sopra citata non esaurisce la molteplicità degli scenari applicativi. Per applicazioni non contemplate nei modelli forniti contattare il referente privacy

Fonti normative e regolamentari di riferimento

Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati D.Lgs. 196/2003 come novellato dal D. Lgs. n. 101/2018 accessibile al seguente indirizzo: https://www.garanteprivacy.it/regolamentoue.

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 G.U. n. 11 del 14 gennaio 2019) accessibili al seguente indirizzo: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069637