



**UNIVERSITÀ DEGLI STUDI DELLA BASILICATA**

**Università degli Studi della Basilicata**

**Piano di Adeguamento al Regolamento Europeo 2016/679**

**GDPR  
(Piano privacy)**

**ESTRATTI**

**Cap. 6 – TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO**

**Cap. 7 - RICERCA SCIENTIFICA E STATISTICA**

## 6. Trasferimento di dati personali all'estero

Con riferimento ai trasferimenti internazionali di dati personali, il GDPR formalizza e amplia il numero di strumenti di trasferimento alternativi al consenso dell'interessato, come le clausole contrattuali tipo, affinché con il trasferimento siano impregiudicati i livelli di protezione delle persone fisiche garantite dal GDPR (art. 44).

La presente sezione ha come obiettivo quello di fornire indicazioni sui fattori da prendere in considerazione al momento del trasferimento dei dati personali verso un paese terzo extra UE o un'organizzazione internazionale, assicurando la continuità del livello di protezione che segue i dati, "attaccata" ai dati (*sticky regulation*), anche successivamente ad un ulteriore trasferimento. Ciò che occorre avere presente è che i trasferimenti verso paesi esteri, in linea di principio, non sono consentiti, sempre che intervengano specifiche garanzie, elencate in ordine gerarchico nel Regolamento, che includono le decisioni di adeguatezza e le deroghe in specifiche situazioni.

Il trasferimento verso paesi terzi è, pertanto, considerato un trattamento ad alto rischio per le libertà e i diritti fondamentali e può avere luogo solo nel rispetto delle condizioni di cui al Capo V del GDPR, sia che riguardino progetti di ricerca, mobilità del personale e degli studenti, richieste di dati provenienti da paesi terzi (per esempio inerenti il *curriculum* di laureati o dipendenti dell'Ateneo), l'utilizzo di piattaforme che non garantiscono la collocazione dei *data center* su territorio UE e altre casistiche piuttosto frequenti in ambito universitario.

Con il GDPR le decisioni di adeguatezza possono essere revocate e, in condizioni particolari, anche in tempi molto brevi per cui nei casi di movimenti della scena politica del paese di destinazione che potrebbero inficiare i presupposti di adeguatezza, su cui si fonda una decisione esistente, e siano già osservabili al momento di avviare un trasferimento, si potrebbe preferire il ricorso a specifiche garanzie. In questo caso, infatti, il trasferimento troverebbe una base di legittimità che prescinde dalla presenza della decisione stessa e quindi dalla sua eventuale revoca.

Per approfondimenti sul trasferimento di dati all'estero si rinvia all'**Allegato n. 6**.

## 7. Ricerca scientifica e statistica

### 7.1 Premessa

Le attività di ricerca scientifica presentano una significativa complessità sotto il profilo della disciplina e degli adempimenti in materia di trattamento di dati personali.

I motivi di tale complessità risiedono, in particolare, nelle caratteristiche delle attività di ricerca, nella natura dei dati trattati, nei peculiari ruoli e compiti riservati ai ricercatori universitari e a eventuali partner di ricerca, spesso destinatari di dati pseudonimizzati (tra cui: altre università, enti, società scientifiche, nonché altri ricercatori che operano anche all'estero).

Da qui la necessità, da parte dell'Università degli Studi della Basilicata, di prestare particolare attenzione al trattamento dei dati personali e di adottare delle strategie orientate a fornire strumenti utili, come ad esempio:

- condividere le buone pratiche adottate o adottabili nell'ambito della ricerca storica, scientifica e statistica al fine di garantire una maggiore protezione dei dati personali e aderenza al GDPR;
- affrontare i temi e/o gli aspetti che presentano maggiori criticità e/o perplessità, anche con l'obiettivo di sottoporre eventuali dubbi interpretativi al Garante per la Protezione dei dati personali o, laddove possibile, fornire alcuni strumenti operativi a tutte le Strutture.

### 7.2 Finalità e ambito applicativo

Se da un lato nel GDPR e nella legislazione interna, nel rispetto dei tempi della ricerca, sono previste misure di semplificazione in ambito di ricerca storica, scientifica e/o statistica, dall'altro è necessaria l'adozione di misure idonee a prevenire possibili violazioni dei diritti degli interessati.

La sostituzione del nominativo dell'interessato con un codice e la conservazione dell'associazione "nominativo – codice" in un archivio separato - il cui accesso è limitato a un numero esiguo di ricercatori (operazione c.d. di "pseudonimizzazione"), ad esempio, è una misura necessaria per garantire il rispetto della normativa in materia di protezione dei dati personali, ma non consente al Titolare di ritenere che il dato trattato sia anonimo.

Largamente diffusa è l'errata convinzione secondo la quale il dato pseudonimizzato (che richiede il rispetto delle norme in materia di protezione dei dati personali) coincida con il dato anonimo (per il quale, non potendo risalire all'identità del partecipante, neanche in via indiretta, non si è tenuti al rispetto del GDPR).

La forte spinta verso gli *OpenData*, anche in ambito di ricerca, può facilmente far riflettere sulla possibilità che lo sviluppo di sofisticate tecnologie consenta la potenziale "re-identificazione" di un interessato i cui dati non siano stati resi del tutto anonimi.

Un altro aspetto rilevante nell'ambito della ricerca storica, scientifica e statistica è inoltre il rispetto del principio di finalità.

Spesso, infatti, non è possibile individuare pienamente le finalità specifiche del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati.

Una semplificazione importante su tale aspetto è prevista espressamente nel GDPR che prevede la possibilità che gli interessati prestino il proprio consenso a determinati settori della ricerca scientifica nel rispetto delle norme deontologiche riconosciute in tale ambito (cfr. considerando n. 33 del GDPR).

### 7.3 Presupposti dei trattamenti

Al fine di agevolare il trattamento dei dati personali finalizzati alla ricerca, può essere utile prevedere alcune strategie di protezione dei dati che frequentemente si possono adottare in ambito universitario, come ad esempio:

- garantire il rispetto del principio della minimizzazione dei dati (evitando di raccogliere informazioni che non sono necessarie per il perseguimento delle finalità della ricerca);
- informare gli interessati sull'uso di propri dati personali nell'ambito del progetto di ricerca (fornendo tutte le informazioni previste dall'articolo 13 del GDPR, salvo i casi d'esenzione che si affronteranno nei prossimi paragrafi);
- predisporre adeguate misure tecniche e organizzative per garantire la protezione dei dati, a seguito di un'accurata analisi dei rischi.

### 7.4 Avvio di un progetto di ricerca

I ricercatori che intendono avviare un progetto devono conoscere i rischi sottesi al trattamento dei dati al fine di evitarli e richiedere, qualora necessaria, una "valutazione d'impatto" (così come avviene ai sensi dell'articolo 35 del GDPR per particolari categorie di dati).

I principi di protezione dei dati non si applicano a informazioni anonime, vale a dire 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.

La valutazione dell'impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;

- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

#### **DESCRIZIONE SISTEMATICA DEI TRATTAMENTI E DELLE FINALITÀ**

Il ricercatore, prima dell'avvio di una ricerca, deve essere in grado di:

- individuare l'ambito, il contesto e le finalità della ricerca;
- effettuare una descrizione accurata del processo, con particolare riferimento alle operazioni di raccolta dei dati;
- effettuare una valutazione dei rischi per i diritti e le libertà degli interessati, anche sulla base delle caratteristiche degli interessati;
- prevedere, anteriormente alla raccolta, le eventuali modalità di comunicazione e diffusione dei dati personali, nonché rilevare le criticità che potrebbero derivare dal trasferimento dei dati all'estero;
- determinare i soggetti coinvolti nel trattamento e individuare le responsabilità a essi associate.

#### **VALUTAZIONE DELLA LEGITTIMITÀ, NECESSITÀ E PROPORZIONALITÀ DEI TRATTAMENTI**

Il ricercatore dovrà individuare le modalità per garantire la legittimità della raccolta ed elaborazione dei dati personali, nonché individuare le misure per garantire l'attuazione dei principi di necessità e proporzionalità dei trattamenti (determinando, tra gli altri aspetti, anche il periodo di conservazione/registrazione dei dati personali).

#### **VALUTAZIONE MISURE PREVISTE PER AFFRONTARE I RISCHI**

Il ricercatore dovrà identificare i beni e gli strumenti tramite i quali sono elaborati e/o archiviati i dati personali (*hardware, software, reti, persone, canali di trasmissione cartacea, etc.*), effettuare l'analisi dei rischi nonché descrivere le misure previste per affrontare i rischi sottesi al trattamento.

L'**Allegato 7** è una scheda mediante la quale il ricercatore può documentare le scelte effettuate, nell'ambito di un progetto di ricerca, per favorire la protezione dei dati personali e la tutela dell'interessato e/o da utilizzare per permettergli di svolgere l'analisi di gran parte degli aspetti contemplati nella materia in oggetto.

#### **7.5 Informativa e consenso in ambito di ricerca**

Il supporto ai ricercatori passa anche dalla previsione di strumenti operativi che gli consentano di informare adeguatamente eventuali partecipanti alla ricerca in merito al trattamento dei loro dati.

Tale presupposto vale anche nel caso in cui siano raccolti dati che non identificano direttamente l'interessato (ad esempio dati che non contengono il nominativo della persona).

La raccolta di dati personali, anche quando inerenti a dati cifrati o pseudonimizzati, deve essere preceduta da un'informativa.

La messa a disposizione di informative adeguate e la raccolta dei consensi secondo le disposizioni vigenti in materia di tutela dei dati personali è:

- un presupposto di legittimità per lo svolgimento del progetto di ricerca in cui è prevista la raccolta;
- condizione per l'eventuale successiva conservazione dei dati al fine di procedere legittimamente a una loro ulteriore utilizzazione (ad esempio, per nuove ricerche o studi nell'ambito di altri progetti o per consentire un legittimo sfruttamento dei risultati delle ricerche stesse, a meno dei casi di esenzione previsti dal GDPR).

Oltre alle informazioni di cui all'art. 13 del GDPR, che sono quelle da fornire qualora i dati personali siano raccolti presso l'interessato, nell'informativa è sempre opportuno informare l'interessato rispetto alla possibilità che i dati personali possano essere conservati e trattati (anche) per scopi statistici o scientifici.

### 7.6 Dati raccolti presso l'interessato

La raccolta presso l'interessato dei dati necessari per lo sviluppo di una ricerca ha l'importante vantaggio di poter rendere l'informativa tempestivamente, fornendo al partecipante tutti i chiarimenti utili. Se previsto, occorre acquisire il consenso.

### 7.7 Dati acquisiti presso terzi

Il fatto che vi siano dati personali resi disponibili da un soggetto terzo (es: una scuola, un'agenzia interinale, etc.) non ne implica la libera utilizzazione o diffusione da parte di un ricercatore.

Il ricercatore dovrà in ogni caso valutare se l'utilizzazione e la pubblicazione di un dato personale a fini di ricerca possa essere effettuata senza che vi sia una ragionevole aspettativa dell'interessato in merito all'ulteriore utilizzo dei propri dati per finalità scientifiche.

Nell'ambito di attività di natura didattica e/o di ricerca proprie dell'Università degli Studi della Basilicata e svolte, per convenzione, presso scuole e/o strutture sanitarie, è possibile che un dato raccolto da tali enti sia poi utilizzato, seppur in forma pseudonimizzata, nell'ambito di attività proprie dell'Ateneo.

L'articolo 14 del GDPR, che fa riferimento alle informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato, esonera l'Università dal rendere un'informativa specifica agli interessati (i cui dati potrebbero essere stati raccolti, ad esempio, da una scuola per finalità diverse da quelle di ricerca), a patto che risulti impossibile o comporti uno sforzo sproporzionato contattare l'interessato e, comunque, a condizione che esistano adeguate misure di salvaguardia.

È importante, tuttavia, che in tal caso le informazioni (di cui all'art. 13 del GDPR) siano comunque rese pubbliche, anche mediante pubblicazione sui siti istituzionali.

In base all'analisi svolta dagli atenei che ospitano Corsi di Laurea in Medicina e Chirurgia, è stato possibile evidenziare che, in particolare, nell'ambito di un rapporto di collaborazione tra università e azienda ospedaliera di riferimento vi siano, in relazione ai dati trattati per specifici progetti di ricerca, differenti e specifiche situazioni.

Ad esempio, potrebbero esistere:

- attività di ricerca proprie dell'Ateneo svolte (anche) tramite personale e strumenti delle strutture sanitarie;
- attività di ricerca proprie delle strutture sanitarie per le quali si utilizzano (anche) personale o strumenti d'Ateneo;
- progetti di ricerca in cui le decisioni sulle modalità e gli strumenti possono essere prese congiuntamente da Ateneo e struttura sanitaria;
- casi, come le sperimentazioni di farmaci, in cui le finalità, le modalità e gli strumenti di trattamento sono decisi in modo distinto dalla società farmaceutica (sia essa committente o sponsor) e dall'Università oppure casi in cui tali decisioni sono prese congiuntamente.

### 7.8 Elaborazione dei dati a fini di ricerca statistica o scientifica

La valutazione dei rischi connessi al trattamento di dati personali deve tenere conto dell'impatto che potrebbe comportare.

Se l'impatto è rilevante, l'attenzione alle misure di protezione dei dati e alle garanzie da riservare all'interessato deve essere alta.

Le garanzie da adottare consistono:

- in una rigorosa limitazione della quantità di dati raccolti;
- nell'immediata cancellazione dei dati identificativi dopo il loro utilizzo;
- nell'adozione di misure tecniche e organizzative volte a garantire che i dati non possano essere utilizzati per adottare decisioni, intraprendere altre azioni riguardo alle persone o essere acquisite da soggetti non autorizzati ("separazione funzionale" come spesso avviene in un contesto di ricerca);
- nell'utilizzo di tecniche di anonimizzazione;

- in un'immediata aggregazione dei dati;
- nel diritto generale e incondizionato di revoca (“*opt-out*”);
- nella pseudonimizzazione e nella cifratura di dati personali in fase di conservazione o di transito.

Tali misure devono essere adottate per ridurre la probabilità di ingerenze negli interessi o nei diritti e nelle libertà fondamentali degli Interessati.

### 7.9 Conservazione dei dati a fini di ricerca statistica o scientifica

Uno dei cambiamenti radicali, apportati dal GDPR, nel settore della ricerca riguarda, essenzialmente, i limiti generali imposti per la conservazione.

Infatti, la conservazione di dati personali raccolti per altre finalità come ad esempio didattica, cura, etc., sarebbe consentita nel rispetto dei limiti imposti dalle norme vigenti, qualora quegli stessi dati venissero dirottati sulla ricerca.

La legittimità della conservazione in ambito scientifico non deve, tuttavia, distrarre dalla necessità di conservare solo i dati pertinenti e non eccedenti e dal curare l'integrità e l'accuratezza in fase di conservazione. I dati personali archiviati nel tempo costituiranno, infatti, il presupposto scientifico sul quale si potranno fondare alcune ipotesi di ricerca statistica, scientifica o storica e sulla base dei quali potrebbe essere verificata l'attendibilità della ricerca stessa e l'autenticità dei risultati.

La corretta conservazione dei dati, quindi, non è soltanto necessaria per adempiere alla normativa in materia di protezione dei dati personali, ma costituisce un requisito fondamentale per garantire professionalità, rigore e accuratezza nell'attività di ricerca.

### 7.10 Dati conservati presso terzi

La corretta conservazione dei dati personali archiviati e/o trattati in formato elettronico deve avvenire tramite strumenti idonei a preservare i dati dal rischio di distruzione o perdita – anche accidentale - nonché dall'accesso abusivo da parte di terzi.

Sebbene, ad esempio, siano innegabili i vantaggi dell'uso del *cloud repository*, in termini di sicurezza, l'Università degli Studi della Basilicata deve prestare attenzione alle implicazioni derivanti dalla conservazione dei dati tramite servizi in *cloud* di terze parti.

L'archiviazione, ad esempio su Google Drive, Dropbox, Onedrive, di interviste audio-video raccolte dai ricercatori, seppur temporaneamente e con il solo obiettivo di trasferire i dati ad un partner di ricerca o di condividere uno spazio di lavoro, comporta un trattamento di dati personali da parte di terzi che offrono il servizio.

Tali soggetti, se ne ricorrono i presupposti devono essere specificamente contrattualizzati come “Responsabili esterni del trattamento”.

Questo aspetto è affrontato anche nella guida “*Cloud Computing - Proteggere i dati per non cadere dalle nuvole*”<sup>12</sup>, a cura del Garante per la protezione dei dati personali, nella quale si precisa espressamente che il “titolare del trattamento” dei dati personali (nella fattispecie Università degli Studi della Basilicata) deve procedere a designare il fornitore dei servizi in cloud “Responsabile esterno del trattamento” e prestare molta attenzione a come saranno utilizzati e conservati i dati personali caricati sulla “nuvola” poiché, in caso di violazioni commesse dal fornitore, anche l'Università potrebbe essere chiamata a rispondere dell'eventuale illecito trattamento.

Ulteriore attenzione deve essere poi prestata a quei fornitori di *cloud repository* che dichiarano di conservare i dati in uno Stato extraeuropeo e/o che prevedono il trattamento degli stessi all'estero, soprattutto qualora l'ordinamento del Paese di destinazione o di transito dei dati non assicuri un adeguato livello di tutela, come chiarito meglio nel seguente paragrafo.

Per garantire che i dati di ricerca siano “al sicuro”, è altresì importante curare non solo i rapporti con il fornitore e verificare come avviene la conservazione dei dati, ma anche curare le misure di protezione e le modalità con cui sono trasmessi (ad esempio adottando opportune tecniche di cifratura).

<sup>12</sup> Sito del Garante per la protezione dei dati personali, doc web n. 1894503.

### 7.11 Trasferimento dei dati all'estero

Nel GDPR vige il principio secondo il quale il trasferimento dei dati personali oggetto di un trattamento verso un paese terzo avviene soltanto se il titolare del trattamento e i responsabili rispettino le condizioni dettate dal Regolamento.

A titolo esemplificativo, e non esaustivo, il trasferimento dei dati può lecitamente avvenire se:

- esiste una decisione di adeguatezza da parte della Commissione europea (perché ritiene che il paese destinatario offra un livello adeguato nella protezione dei dati);
- sono adottate clausole contrattuali standard;
- si fa riferimento alle norme vincolanti di impresa cioè alle BDR (che consentono il trasferimento all'interno della società se il regime è stato preventivamente approvato da un Garante europeo);
- si fa riferimento a codici di condotta e certificazione;
- sono state inserite particolari disposizioni in accordi amministrativi;
- ci sono state sentenze di un'autorità giurisdizionale o amministrativa, purché basati su un accordo internazionale se c'è stato il consenso dell'interessato.

### 7.12 Diffusione dei dati a fini di ricerca scientifica o statistica

Soprattutto nell'ambito di progetti europei, è richiesto al ricercatore di stimolare il dialogo e il dibattito sui risultati della ricerca scientifica, garantendo il diritto all'informazione ad un pubblico più vasto ed eterogeneo, rendendo le conoscenze acquisite più attrattive per i giovani, aumentando l'interesse della società per l'innovazione scientifica e lo sviluppo tecnologico.

Sebbene in alcuni casi, nel rispetto dell'essenzialità dell'informazione, il ricercatore possa evitare di diffondere risultati scientifici che includano riferimenti (anche indiretti) a persone fisiche, in altri casi è importante farlo poiché:

- l'informazione, anche dettagliata, può risultare indispensabile per lo sviluppo delle tesi di ricerca e dei risultati ottenuti, nonché per la qualificazione degli interessati e di ciò che rappresentano;
- si tratta di una richiesta espressa degli stessi interessati (eventualmente volta a valorizzare il loro coinvolgimento in un'attività di ricerca);
- si tratta di interviste riguardanti circostanze o fatti già resi noti da altre fonti di informazione.

La divulgazione di risultati scientifici contenenti dati personali, se di rilevante interesse pubblico o sociale, non si pone in contrasto con il rispetto della sfera privata dell'interessato a patto che lo stesso sia stato adeguatamente informato in merito alla diffusione di proprie informazioni.

Si precisa, tuttavia, che il ricercatore deve sempre svolgere una valutazione di proporzionalità nella diffusione di dati personali e sull'opportunità di provvedere alla loro stessa diffusione a particolari categorie di interessati. Ad esempio, al fine di tutelare i diritti degli interessati, il ricercatore non deve pubblicare i nomi di minori coinvolti in progetti di ricerca qualora il prodotto che si intenda diffondere (articolo scientifico, video, etc.) non dia positivo risalto al minore e/o nel caso in cui la pubblicità dei suoi dati possa, in futuro, arrecargli un danno alla sua personalità. Resta fermo l'obbligo per il ricercatore di acquisire l'immagine o le informazioni, in un quadro di assoluta trasparenza, nonché di valutare, volta per volta, eventuali richieste di opposizione da parte dell'interessato.

## 8. Priorità e relative azioni organizzative e tecniche

Analizzato il contesto interno all'Ateneo sulle questioni attinenti alla protezione dei dati personali, considerata la necessità di procedere in maniera sistemica alle attività di adeguamento, sono state individuate le seguenti prioritarie misure/azioni di carattere sia tecnico che organizzativo, ritenute adeguate e concorrenti per la conformità al GDPR e al Codice.