Aspetti Privacy

Si riportano di seguito alcuni richiami essenziali ed operativi, anche per la predisposizione.

I seguenti richiami sono da intendersi necessariamente a carattere indicativo e si invita comunque ciascuna Coordinatrice/Coordinatore di progetto a far costante riferimento a disposti normativi in materia di privacy di cui al Regolamento (UE) 2016/679 (GDPR).

Ogni attività prevista per il rispetto della normative privacy, è infatti rimessa alla responsabilità delle Coordinatrici/Coordinatori di Progetto, prevedendo già la procedura, come riportato nelle dichiarazioni delle schede di presentazione dei progetti (Modello A), che: *"La proposta progettuale non prevede ulteriori oneri a carico del bilancio universitario, salvo i compensi previsti per il personale che vi partecipa,* ***ed è pienamente sostenibile in termini di fattibilità con l'apporto dei soli componenti del gruppo di progetto (non prevede quindi per il suo sviluppo il coinvolgimento di strutture universitarie)****".*

1. Definizione di dato personale (art. 4 GDPR)

Per "dato personale" si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile (l'"interessato"). Una persona è "identificabile" quando può essere individuata, direttamente o indirettamente, anche tramite identificativi come nome, numero di identificazione, dati di ubicazione, identificativi online (es. indirizzo IP, cookie) o elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Principali categorie di dati personali

Dati personali "comuni": a titolo esemplificativo, identificativi e dati di contatto, numeri di identificazione, dati di tracciamento online.

Categorie particolari di dati, "dati sensibili" (art. 9 GDPR): a titolo esemplificativo, dati che rivelano, ad esempio, origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale. Il trattamento è in linea generale vietato, salvo specifiche condizioni (es. consenso esplicito, obblighi di legge in ambito lavoro/sociale, interesse pubblico rilevante).

2. Principi generali di protezione dei dati (art. 5 GDPR)

Ogni trattamento di dati personali deve rispettare i principi di cui all'art. 5 GDPR. In base al principio di responsabilizzazione (accountability), il Titolare non solo deve conformarsi a tali principi, ma deve anche poter dimostrare l'efficacia delle misure adottate.

In particolare, i dati personali devono essere:

Trattati in modo lecito, corretto e trasparente: il trattamento deve basarsi su una valida base giuridica e su informazioni chiare agli interessati.

Raccolti per finalità determinate, esplicite e legittime: è vietato il riutilizzo per scopi incompatibili con quelli dichiarati.

Adeguati, pertinenti e limitati a quanto necessario (minimizzazione): si privilegia, quando possibile, la raccolta di dati non personali o meno dettagliati.

Esatti e aggiornati: vanno previste misure tempestive di rettifica o cancellazione dei dati inesatti, tenendo conto dei rischi che un errore potrebbe comportare per i diritti dell'interessato.

Conservati per un tempo non superiore al necessario: la durata va definita e giustificata; raggiunta la finalità, i dati devono essere cancellati o anonimizzati in modo irreversibile.

Trattati con misure di sicurezza adeguate: misure tecniche e organizzative (es. controllo accessi, cifratura, tracciamento) per prevenire trattamenti illeciti, perdite o danni accidentali.

3. Questionari: regole operative generali

Nella progettazione e somministrazione di questionari occorre porre particolare attenzione alla tutela dei dati dei partecipanti, assicurando che i dati eventualmente raccolti siano trattati nel rispetto del GDPR e, in particolare, dei principi di cui all'art. 5.

Obblighi minimi degli autori/somministratori

Definire con chiarezza finalità e contenuti del questionario (evitando la raccolta di dati non necessari).

Valutare preventivamente se il questionario comporta raccolta di dati personali e, se sì, di quale tipologia (comuni / categorie particolari).

Predisporre adeguate misure di riservatezza e sicurezza per la raccolta e la conservazione dei dati.

Fornire ai partecipanti le informazioni sul trattamento dei dati e sulle misure adottate per tutelarne la privacy, prima della compilazione.

4. Dati anonimi, dati pseudonimizzati e conseguenze

La disciplina in materia di protezione dei dati personali non si applica ai dati anonimi, ossia alle informazioni che, a seguito di un trattamento irreversibile, non possono più essere associate a un individuo specifico.

Il dato anonimo non va confuso con il dato pseudonimizzato: in quest'ultimo caso, il dato personale non è più direttamente attribuibile a un individuo, ma può essere riassociato attraverso informazioni aggiuntive conservate separatamente.

Quando un questionario può dirsi "anonimo"

Un questionario risulta anonimo quando non sussiste, o è minimo, il rischio di identificazione diretta o indiretta dei rispondenti, anche tramite collegamenti successivi con altre informazioni.

Pertanto, se esiste la possibilità ragionevole di risalire al rispondente (direttamente o indirettamente), il questionario non è da considerarsi anonimo.

5. Indicazioni pratiche per questionari in Google Forms

Per ridurre il rischio di identificazione e facilitare l'adozione di un'impostazione anonima, si raccomanda di:

Disattivare la raccolta degli indirizzi e-mail e qualsiasi opzione che registri automaticamente l'identità del rispondente.

Preferire domande a risposta chiusa (es. scelta multipla) rispetto a domande aperte, che possono indurre il rispondente a inserire elementi identificativi.

Evitare combinazioni di domande che, nel complesso, rendano il rispondente riconoscibile (es. struttura/ruolo + sede + informazioni molto specifiche).

6. Informativa privacy (art. 13 GDPR) per questionari non anonimi

Se il questionario non è anonimo e comporta trattamento di dati personali, deve essere resa disponibile ai partecipanti un'Informativa ai sensi dell'art. 13 GDPR prima dell'effettiva compilazione. L'Informativa deve essere chiara, accessibile e trasparente.