PREMESSA

Il Regolamento Generale sulla Protezione dei Dati (General Data Protection Regulation, GDPR, EU 2016/679), uniformando le diverse normative in materia di protezione dei dati, garantisce a tutti i residenti nell'Unione Europea la protezione dei propri dati personali e la tutela della propria riservatezza.

Data l'importanza e la complessità del documento, la Commissione Etica AIP ha elaborato dei quesiti con le relative risposte (FAQ) con l'obiettivo di supportare le associate e gli associati nella comprensione e applicazione del GDPR nelle proprie ricerche.

L'elaborazione delle FAQ ha richiesto un processo caratterizzato da tre fasi distinte. Nella prima fase le FAQ sono state elaborate grazie ad una consulenza giuridica[1]. Nella seconda fase una versione preliminare delle FAQ è stata inviata a tutte le associate e gli associati con la richiesta di fornire un riscontro attraverso la compilazione di un questionario anonimo in relazione alla chiarezza e all'utilità delle FAQ e aggiungendo possibili commenti. In totale hanno risposto 20 socie e soci. Nella terza fase le risposte e i commenti ricevuti sono stati integrati dalla Commissione Etica AIP nelle FAQ e discussi con il referente della consulenza giuridica fino alla redazione della versione finale.

FAQ 1. Cosa si intende per "dato personale"?

Per "dato personale" deve intendersi qualsiasi informazione riguardante una persona fisica identificata o identificabile (ad es. il nome ed il cognome, la data di nascita, il sesso e il genere, il codice fiscale, l'indirizzo di posta elettronica, un'immagine fotografica, ecc.).

La persona fisica alla quale fanno riferimento i dati personali viene individuata quale "soggetto interessato".

Queste informazioni sono un dato personale quando identificano in modo univoco una specifica persona fisica anche attraverso l'incrocio con altri possibili dati.

FAQ 2. Quando un soggetto deve considerarsi identificabile?

Si considera identificabile la persona fisica nel caso in cui i dati raccolti siano riconducibili ad essa in via diretta o indirettamente.

I dati personali, pertanto, possono suddividersi in **dati che permettono l'identificazione diretta del soggetto interessato** - come i dati anagrafici (ad esempio, nome e cognome, il codice fiscale), le immagini, ecc. - e in **dati che permettono l'identificazione indiretta del soggetto interessato** (attraverso l'incrocio dei dati), come un numero di identificazione (ad esempio, l'indirizzo IP, il numero di targa).

Pertanto, se il dato trattato non è idoneo ad identificare in via diretta una determinata persona, il ricercatore dovrà comunque domandarsi se tali dati siano in grado di identificare il partecipante attraverso l'incrocio con altri dati (ad es. anche le semplici iniziali di un soggetto dovranno considerarsi "dati personali" – e quindi sottoposti alla disciplina del GDPR – nel caso in cui

[1] La consulenza, finanziata dall'AIP, è stata prestata dall'avv. Cristiano Michela.

permettano al ricercatore di risalire alle generalità complete del partecipante).

FAQ 3. Cosa si intende per "trattamento di dati personali"?

Il trattamento di dati personali è qualsiasi operazione o insieme di operazioni 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 dei dati personali stessi.

FAQ 4. Chi è il Titolare del Trattamento dei dati personali?

Il Titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità, le modalità ed i mezzi per svolgere un determinato trattamento di dati personali; nel rapporto ricercatore- partecipante, il titolare del trattamento sarà il legale rappresentante dell'ente di ricerca a cui si appartiene (ad esempio, il Rettore in ambito universitario).

Il Titolare del trattamento può designare ai sensi dell'art. 2 quaterdecies del D.Lgs. 101 del 2018 altre figure (ad esempio, i dirigenti e i direttori di dipartimento) ad adottare sotto la propria responsabilità specifici compiti e funzioni connessi al trattamento di dati personali come ad esempio l'individuazione di tutte le misure tecniche e organizzative necessarie per garantire il rispetto del Regolamento UE 2016/679 ("GDPR").

FAQ 5. Chi è il Responsabile del Trattamento dei dati personali?

Ai sensi dell'art. 28 del Regolamento UE 2016/679 ("GDPR"), il Responsabile del trattamento è colui che, esternamente all'Ente di ricerca, effettui un trattamento per conto del titolare del trattamento (es. se un soggetto utilizza un cloud per l'archiviazione dei dati, il responsabile esterno è il gestore della piattaforma utilizzata).

Il Titolare deve ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti del soggetto interessato.

I trattamenti svolti da parte di un responsabile del trattamento sono disciplinati da un contratto che vincoli il responsabile del trattamento al titolare del trattamento e che definisca la materia disciplinata, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di soggetti interessati, gli obblighi e i diritti del titolare del trattamento.

FAQ 6. Cosa si intende per principio dell'accountability?

Con il Regolamento UE 2016/679 ("GDPR") il Titolare del trattamento diventa responsabile della gestione di tutta l'attività di trattamento dei dati personali. In particolare, sarà il Titolare del trattamento a dover decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali in considerazione della specifica realtà nella quale opera.

In particolare, viene imposta a tutti i Titolari una gestione trattamentale responsabile che tenga

conto dei rischi connessi all'attività svolta e che sia idonea a garantire la piena conformità del trattamento dei dati personali ai principi sanciti dal Regolamento UE 2016/679 ("GDPR") e dal D.Lgs. 196 del 2003 novellato dal D.Lgs. 101 del 2018.

FAQ 7. Cosa si intende per "categorie particolari di dati personali"?

Il Regolamento UE 2016/679 ("GDPR") ha eliminato la categoria dei dati c.d. sensibili, sostituita da quella dei dati appartenenti a categorie particolari (c.d. "dati particolari").

I dati personali appartenenti a categorie particolari ex art. 9 GDPR (ex "dati sensibili") sono quei dati idonei a rivelare l'appartenenza etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute (si veda FAQ 8), alla vita sessuale o all'orientamento sessuale della persona (si veda FAQ 9).

Vista la particolare delicatezza di questi dati al ricercatore viene richiesta una maggiore attenzione nell'espletamento dello studio condotto.

FAQ 8. Quali dati comprendono i "dati relativi alla salute"?

I dati relativi alla salute sono tutti quei dati personali particolari 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.

Anche le risposte ad un questionario auto-somministrato sulla salute mentale (per valutare ad esempio l'ansia o la depressione) e i relativi punteggi sono dati particolari relativi alla salute. Tali dati rientrano nella categoria "particolare" di dati di cui all'art. 9 del GDPR nel caso in cui attraverso tali rilevazioni si riesca ad identificare uno specifico partecipante alla ricerca.

FAQ 9. I dati relativi all'orientamento sessuale sono dati particolari (ex dati sensibili)?

Sì, i dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica rientrano nei dati appartenenti a categorie particolari di cui all'art. 9 Regolamento UE 2016/679 ("GDPR") se permettono di identificare il partecipante alla ricerca.

FAQ 10. I dati psicometrici sono elementi caratteristici della identità psichica di un individuo? I dati ricavati da strumenti psicometrici, scale o questionari che rilevano lo stato di salute della persona sono "dati particolari"?

Tutti i dati, compresi quelli comportamentali, che rivelino in modo univoco informazioni connesse allo stato di salute fisica o mentale passata, presente o futura di una persona fisica identificata o identificabile rientrano nell'ambito dei dati relativi alla salute ed il loro trattamento è assoggettato alla speciale disciplina contenuta nell'art. 9 Regolamento UE 2016/679 ("GDPR").

È il ricercatore stesso che deve valutare quando i dati che sta rilevando sono dati relativi alla salute fisica o mentale, e decidere il livello di protezione da assegnare.

Solo nel caso in cui i dati ricavati da strumenti psicometrici, scale o questionari siano in grado di

rilevare l'appartenenza etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale o dati relativi alla salute o alla vita o all'orientamento sessuale del soggetto investigato, sono da considerarsi "dati particolari". A titolo esemplificativo, i dati raccolti attraverso scale psicometriche o altri strumenti di rilevazione come "ansia" "depressione" o "burnout" rientrano nella categoria "particolare" di dati ex art. 9 del Regolamento UE 2016/679 ("GDPR") nel caso in cui attraverso tali rilevazioni si riesca ad identificare (in modo univoco) un partecipante alla ricerca.

FAQ 11. Quando il trattamento ha ad oggetto dati rientranti nella categoria dei dati particolari (cfr. Faq n. 7) occorre innalzare il livello di guardia ed adottare maggiori misure di sicurezza volte a tutelare il dato personale trattato?

Si, il trattamento di dati particolari richiede precauzioni e misure aggiuntive rispetto al trattamento di semplici dati comuni per garantire la protezione e la sicurezza di tali dati, poiché possono rivelare informazioni personali altamente sensibili.

A titolo esemplificativo ma non esaustivo si indicano di seguito alcune delle cautele da adottare nell'ambito di tale trattamento:

Idonea Base Giuridica: occorrerà assicurarsi di avere una base legale adeguata per trattare tali dati. Le basi giuridiche possono includere il consenso esplicito dell'interessato, l'adempimento di obblighi legali, la protezione degli interessi vitali dell'interessato o l'esecuzione di compiti di interesse pubblico o nell'esercizio di pubblici poteri.
Consenso esplicito: se il trattamento non si basa su altre basi legali, è necessario ottenere il consenso esplicito e informato dell'individuo. Il consenso deve essere specifico per il tipo di dati trattati e per la finalità del trattamento.
Finalità Limitate: il trattamento dei dati particolari dovrà essere limitato solo alle finalità specifiche per cui sono stati raccolti. Dovrà essere evitato l'utilizzo di tali dati per altri scopi non autorizzati.
Minimizzazione dei Dati: bisognerà raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità dichiarate. Evitare di raccogliere dati eccessivi o non pertinenti.
Trasparenza: si dovranno fornire informazioni chiare e complete agli interessati riguardo alle finalità del trattamento, alle categorie di dati coinvolti, ai destinatari dei dati, e ai loro diritti.
Sicurezza dei Dati: occorrerà implementare misure di sicurezza adeguate per proteggere i dati particolari da accessi non autorizzati, perdite o alterazioni.
Conservazione Limitata: i dati sensibili dovranno essere conservati solo per il tempo necessario a raggiungere le finalità dichiarate. Una volta che non saranno più necessari i dati particolari dovranno essere cancellati o anonimizzati.
Diritti degli Interessati: sarà necessario garantire che le persone interessate possano esercitare i loro diritti, come il diritto di accesso, rettifica, cancellazione e opposizione al trattamento dei loro dati.
Formazione del Personale: il Titolare del trattamento dovrà provvedere a che il personale coinvolto nel trattamento dei dati sia adeguatamente informato e formato sulla gestione corretta dei dati particolari.
Valutazione d'Impatto sulla Privacy: nel caso in cui il trattamento possa comportare rischi elevati per i diritti e le libertà delle persone, sarà opportuno condurre una valutazione d'impatto sulla privacy (c.d. DPIA) per valutare e mitigare tali rischi.

Trasferimenti Internazionali: nel caso in cui i dati particolari debbano essere trasferiti al di fuori del territorio dell'Unione Europea (nel contesto del GDPR) o da paese a paese, sarà necessario assicurarsi che siano adottate adeguate misure di sicurezza e che vi sia una base legale per il trasferimento.

FAQ 12. Cosa si intende per "base giuridica"?

La base giuridica è una condizione tipica, al verificarsi della quale il trattamento dei dati personali risulta lecito. Ad esempio, se un partecipante fornisce il consenso al trattamento dei dati personali per finalità di ricerca, il trattamento da parte del ricercatore è lecito.

Vi sono tuttavia anche altre condizioni in grado di rendere lecito il trattamento di dati personali come, ad esempio, l'adempimento degli obblighi contrattuali (art. 6 par. 1 lett. b), l'adempimento di un obbligo discendente dalla legge (art. 6 par. 1 lett. c) o il perseguimento di un pubblico interesse (art. 6 lett. e).

Ad esempio, se si è in presenza di un contratto, il trattamento è lecito poiché *"necessario all'esecuzione di un contratto di cui il soggetto interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso"*.

Un ulteriore esempio riguarda la normativa fiscale che impone di conservare la documentazione contabile per 10 anni. Il professionista potrà quindi lecitamente conservare (e quindi trattare) i dati del paziente per tutto quel periodo temporale. Decorsi i 10 anni, non essendoci più una base di liceità, il Titolare del trattamento dovrà interrompere il trattamento di quei dati personali.

Si riporta il link della pagina web del Garante per un approfondimento sul tema in oggetto: https://www.garanteprivacy.it/regolamentoue/fondamenti-di-liceita-del-trattamento

FAQ 13. Cosa si intende per "principio di minimizzazione dei dati"?

A norma dell'art 5 par. 1 lett. c) del Regolamento UE 2016/679 ("GDPR"), il principio di minimizzazione prevede che il Titolare tratti soltanto dati personali *"adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali i dati sono stati raccolti".*

Il ricercatore, pertanto, dovrà evitare di trattare dati personali "eccedenti" (e quindi non indispensabili) per il raggiungimento delle finalità che si è prefissato attraverso il progetto di ricerca.

FAQ 14. Cosa si intende per "dati biometrici"?

I dati biometrici sono 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 (impronte digitali) (art. 4, par. 1, n. 14). Occorre precisare che le videoregistrazioni e le audioregistrazioni non rientrano nella categoria dei dati biometrici così come stabilito dal Garante in un recente provvedimento avente ad oggetto il riconoscimento dei partecipanti a dei corsi di formazione in diretta streaming (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6826368). Perché si possa parlare di trattamento di dati biometrici, occorre che la verifica dell'identità sia automatizzata, tramite l'ausilio di appositi strumenti software o

hardware.

FAQ 15. Come trattare i dati biometrici?

Qualora il trattamento compiuto riguardi i dati biometrici, il Titolare del trattamento dovrà predisporre (prima di iniziare il trattamento) delle misure tecniche ed organizzative più stringenti idonee ad assicurare la salvaguardia dei diritti e delle libertà fondamentali dei soggetti interessati (es. cifratura o pseudonimizzazione).

FAQ 16. È sempre necessario il consenso al trattamento dei dati relativi alla salute?

No. Nel caso in cui il trattamento venga effettuato con finalità di cura (prestazione sanitaria), i dati personali relativi alla salute potranno essere trattati lecitamente in forza della base giuridica disciplinata dall'. 9, par. 2, lett. h) e par. 3 del GDPR. Questo trattamento deve essere effettuato da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza.

Resta ferma la necessaria acquisizione del consenso al trattamento dei dati per finalità non di cura, in ossequio a quanto previsto dalle regole deontologiche emanate dal Garante delle privacy il 19 dicembre 2018 (reperibili al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069677).

FAQ 17. Il Consenso al trattamento dei dati e il Consenso informato sono la stessa cosa?

No, sono documenti con contenuti diversi e redatti per finalità differenti.

Il consenso al trattamento dei dati è una delle molteplici basi giuridiche che rendono lecito il trattamento dei dati personali.

Il consenso informato, invece, non trae origine dal GDPR ma è regolato direttamente dalla dichiarazione di Helsinki relativa ai principi etici per la ricerca che coinvolge i soggetti umani emanata ad ottobre 2013, come richiamato dal Codice Etico. Tale consenso permette al partecipante di "avere informazioni su scopi, metodi, provenienza dei fondi e conflitti di interesse, affiliazioni istituzionali dei ricercatori coinvolti, benefici attesi e potenziali rischi dello studio, disagi che potrebbe comportare, disposizioni post-studio e qualsiasi altro aspetto rilevante dello studio stesso".

FAQ 18. Dati del minore, fino a che età serve il consenso dei genitori?

Qualora il consenso costituisca la base giuridica del trattamento dei dati del minore (ad esempio per finalità di ricerca), questo deve essere espresso da entrambi i genitori (o dal tutore legale) fino al raggiungimento della maggiore età (18 anni).

L'abbassamento della soglia di età operato dall'art. 8 par. 1 Regolamento UE 2016/679 riguarda esclusivamente il consenso al trattamento dei dati personali del minore raccolti nell'ambito dell'offerta diretta di servizi della società dell'informazione (ad es. social media).

FAQ 19. L'art. 2 – quinquies d.lgs. 196/03, che ha abbassato a 14 anni l'età minima per prestare il consenso, riguarda tutti i trattamenti di dati personali del minore?

No, l'art. 2-quinquies co.1 d.lgs. 196/2003 (così come novellato dal d.lgs. 101/2018) dispone che il minore quattordicenne può esprimere il consenso al trattamento dei propri dati personali in attuazione dell'articolo 8, paragrafo 1, del Regolamento UE 2016/679. Si applica esclusivamente ai trattamenti dei dati raccolti nell'ambito dell'erogazione dei servizi della società dell'informazione e non a tutti gli altri trattamenti.

Quindi, qualora il consenso costituisca la base giuridica del trattamento dei dati del minore per finalità di ricerca, questo deve essere espresso da entrambi i genitori (o dal tutore legale) fino al raggiungimento della maggiore età (18 anni).

FAQ 20. Nelle ricerche con minori che prevedono la compilazione di moduli online come si deve raccogliere il consenso dei genitori?

Il Regolamento UE 2016/679 ("GDPR") non prevede specifiche modalità pratiche per raccogliere il consenso dei genitori del minore; pertanto, in ossequio al principio di accountability, spetta al titolare del trattamento porre in atto le misure adeguate per accertarsi che il consenso sia prestato o autorizzato da entrambi i genitori.

Il Titolare sarà tenuto a provare di aver acquisito il consenso al trattamento da parte degli esercenti la responsabilità genitoriale e pertanto occorrerà inviare loro il modulo dell'informativa sulla privacy e la richiesta di consenso che dovranno essere rispediti sottoscritti, anche con modalità telematiche.

Tali documenti, pertanto, si potranno quindi ottenere anche con uno scambio conforme di email.

Nel caso in cui i genitori non possiedano strumenti telematici di trasmissione o nel caso in cui l'indirizzo e-mail da loro fornito non sia a loro immediatamente riconducibile, il titolare, qualora si serva di piattaforme di video-conferenza, potrà anche registrare o video-registrare la sua spiegazione circa le finalità della ricerca e le modalità adottate per il trattamento dei dati personali richiedendo il consenso a quel particolare tipo di trattamento.

FAQ 21. Nel caso in cui una scuola abbia inserito nel proprio PTOF (Piano Triennale dell'Offerta Formativa) la realizzazione di indagini con gli alunni, è necessario richiedere autorizzazione ai genitori?

Il fatto che sul PTOF venga inserita la realizzazione di un'indagine su soggetti minorenni non esonera il Titolare del trattamento dal provvedere a raccogliere tutti i necessari consensi da parte degli interessati (e/o le autorizzazioni dei genitori dei minori partecipanti alla ricerca) prima di effettuare il trattamento programmato.

FAQ 22. Per le ricerche con dati anonimi o anonimizzati, si applica la disciplina sulla protezione dei dati personali di cui al Regolamento UE 2016/679 ("GDPR")?

I dati originariamente non associabili ad una persona fisica identificata o identificabile (dati

anonimi) oppure che sono stati resi interamente anonimi (anonimizzati), in modo tale che la persona fisica non sia o non sia più identificabile, **NON** sono considerati dati personali.

Il Regolamento UE 2016/679 ("GDPR") non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca (così come previsto dal considerando 26 del Regolamento UE 2016/679).

FAQ 23. Cosa si intende per anonimizzazione?

L'anonimizzazione è quell'operazione di de-identificazione mirata a trasformare irreversibilmente i dati personali in dati anonimi.

Per anonimizzare i dati, vengono applicate diverse tecniche che possono includere la rimozione o l'alterazione di informazioni identificabili, come nomi, indirizzi, numeri di telefono o dati biometrici. L'obiettivo è quello di trasformare i dati in una forma tale che non sia possibile risalire all'identità dell'individuo originale.

L'anonimizzazione deve essere tuttavia irreversibile: l'informazione originariamente non associabile ad uno specifico soggetto interessato (c.d. dato anonimo) può divenire "dato personale" allorché, attraverso una successiva operazione di collegamento ad informazioni di diversa natura, risulti comunque idonea a rendere identificabile un soggetto.

Non rientrano nella categoria dei dati anonimi o anonimizzati i dati che, ancorché raccolti in forma anonima, incrociati con altre informazioni (es. informazioni socio- anagrafiche o demografiche) potrebbero rilevare l'identità delle persone fisiche a cui si riferiscono.

In conclusione tutto ciò che non rientra nella categoria dei dati anonimi e/o anonimizzati dovrà essere trattato secondo le regole e le cautele esemplificate nelle FAQ precedenti.

FAQ 24. Ricerche condotte su dati anonimi, devo raccogliere il consenso al trattamento dei dati personali?

No, per la raccolta di dati anonimi non è necessario acquisire il consenso al trattamento dei dati.

FAQ 25. Raccolta dei dati anonimi relativi ai minori, bisogna acquisire il consenso dei genitori?

No, i dati anonimi non permettono di identificare una persona fisica (maggiorenne o minorenne che sia) e pertanto non rientrando nella disciplina del Regolamento UE 2016/679 e non sarà necessario raccogliere il consenso al trattamento dei dati da parte dei genitori.

È bene tenere presente che il Codice Etico AIP prevede di raccogliere invece il consenso alla partecipazione alla ricerca, sia che i dati raccolti siano anonimi o no

FAQ 26. Cosa si intende per "ricerche con dati pseudonimizzati"?

Ai sensi dell'art. 4 par. 1 n. 5 del Regolamento UE 2016/679 la "pseudoanonimizzazione" è un processo in cui i dati personali vengono trasformati in modo da ridurre il rischio di identificazione

diretta degli individui, ma consentendo comunque la possibilità di ricongiungere i dati con ulteriori informazioni per identificare le persone coinvolte (c.d. informazione di riconciliazione o chiave de-pseudoanonimizzazione").

Queste informazioni aggiuntive sono di solito detenute da un soggetto separato o da un sistema di gestione dei dati che può collegare i dati pseudonimizzati ai dati personali originali solo in determinate circostanze, ad esempio, in caso di necessità legale o per scopi di ricerca.

Esempi di dati "pseudonimizzati" nelle ricerche di psicologia sono: ricerche ove i dati personali sono stati preventivamente codificati così da non permettere al singolo ricercatore di abbinare il codice trattato ad uno specifico partecipante. Tali dati, tuttavia, non potranno ritenersi anonimi e quindi esclusi dalla disciplina del GDPR posto che, attraverso un'attività di decodifica, potranno essere ricondotti ed assegnati ai vari partecipanti alla ricerca (abbinamento delle iniziali M.R. all'elenco dei partecipanti che permette di assegnare il nome Mario Rossi a tale codice).

FAQ 27. Nel caso di dati pseudonimizzati, devo raccogliere il consenso al trattamento dei dati personali?

Sì, è necessario raccogliere il consenso al trattamento dei dati pseudonimizzati poiché rientrano nella definizione di "dati personali" e sono assoggettati alla relativa disciplina normativa.

FAQ 28. Relativamente ai dati pseudonimizzati, trova applicazione la disciplina sulla protezione dei dati personali di cui al Regolamento UE 2016/679 ("GDPR")?

I dati personali sottoposti a de-identificazione, cifratura o pseudonimizzazione, che possano essere tuttavia utilizzati per re-identificare una persona, rimangono dati personali e rientrano nell'ambito di applicazione del Regolamento UE 2016/679 ("GDPR"). Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Ciò può avvenire anche solo mediante utilizzo o incrocio di informazioni o altri dati.

FAQ 29. In cosa consiste la de-identificazione?

De-identificare significa eliminare la correlazione tra i dati personali e una determinata persona fisica interessata, rendendo impossibile l'identificazione della stessa.

A titolo esemplificativo immaginando di avere un set di dati contenente informazioni mediche di pazienti, come diagnosi, trattamenti e risultati dei test per de-identificare questi dati si potrebbe ipotizzare di rimuovere i nomi dei pazienti e sostituirli con identificatori univoci, aggregare le diagnosi per categorie più ampie senza dettagli specifici e rimuovere informazioni di dettaglio come i codici univoci associati al paziente.

FAQ 30. In cosa consiste la cifratura?

I sistemi di cifratura possono agire per "trasposizione" (mescolando i caratteri di un messaggio in un nuovo ordine) o per "sostituzione" (sostituendo un carattere con un altro carattere secondo

una regola specifica), o una combinazione di entrambi.

Attraverso un codice di decodifica sarà possibile far tornare “in chiaro” il dato precedentemente anonimizzato.

Ad esempio, in una cifratura per trasposizione “Mario Rossi” può diventare “iramo siros”; in una sostituzione “Mario Rossi” può diventare “m2r1014 r14ss10”.

FAQ 31. Perché pseudonimizzare un dato personale?

L’applicazione della pseudonimizzazione ai dati personali deve essere considerata una misura di sicurezza in quanto permette di ridurre i rischi per i soggetti interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. Rientra pertanto tra una delle misure di sicurezza richiamate dall’art. 32 del Regolamento UE 2016/679 (“GDPR”).

FAQ 32. Nel caso di ricerca storica su perizie criminologiche, come deve essere il trattamento dei dati?

Il trattamento deve essere effettuato nel rispetto delle “*Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica*”.

Per maggiori approfondimenti si riporta di seguito il link alla pagina web del Garante:

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069661

FAQ 33. Possono essere utilizzati i dati raccolti prima dell’entrata in vigore del Regolamento UE 2016/679 (“GDPR”)?

Si, ma è necessario valutare la corretta individuazione delle basi giuridiche del trattamento, aggiornare – ove necessario – le informative e verificare che vi siano le necessarie misure di sicurezza richieste dal GDPR per la tutela dei dati personali trattati nel corso della ricerca.

FAQ 34. Cosa è necessario fare per individuare correttamente le basi giuridiche del trattamento di dati già raccolti?

Va innanzitutto ricordato che la corretta individuazione delle basi giuridiche del trattamento di dati già raccolti è fondamentale per garantire la conformità alle leggi nazionali e sovrannazionale sulla protezione dei dati.
Per una corretta valutazione delle basi giuridiche sottese al trattamento bisognerà:

- esaminare le finalità per le quali sono state raccolti i dati. Ogni trattamento deve avere una finalità specifica e legittima;
- conoscere le basi giuridiche declinate nel GDPR come ad esempio il consenso dell'interessato, l'adempimento di un contratto, l'adempimento di obblighi legali, la protezione degli interessi vitali dell'interessato, l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri, e così via;
- verificare quale di queste basi è la più pertinente al trattamento specifico. Ad esempio, se

viene fornito un servizio per il quale è necessario trattare i dati dell'utente, la base giuridica potrebbe essere l'adempimento di un contratto. Nel caso in cui il trattamento si basi sul consenso occorrerà verificare se il consenso sia stato ottenuto in modo chiaro, specifico e informato. Se il trattamento è necessario per adempiere un obbligo legale a cui si è soggetti, bisognerà essere in grado, ad esempio, di dimostrare che quel trattamento sia strettamente correlato a tale obbligo.

FAQ 35. In ricerche che prevedano l'uso di video-registrazioni e/o audio-registrazioni, devo acquisire un consenso al trattamento dei dati?

Il consenso al trattamento dei dati è sempre obbligatorio in caso di video-registrazioni, mentre in caso di audio-registrazioni il consenso è necessario solo se non risultino anonime (e quindi il vocale non sia riconducibile ad un dato partecipante).

FAQ 36. Cosa accade in caso di trattamento non corretto o violazione dei dati personali (cd. DATA BREACH)?

In caso di violazione dei dati personali è obbligatorio (salvo alcune eccezioni) informare il Garante privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui si è venuti a conoscenza della violazione. La notifica deve descrivere la natura della violazione dei dati personali e descrivere le probabili conseguenze della violazione, nonché le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e per attenuare i possibili effetti negativi.

Queste violazioni possono verificarsi a causa di varie ragioni, tra cui:

- Attacchi informatici: Un hacker o un gruppo di hacker può penetrare nei sistemi informatici di un'organizzazione al fine di accedere e ottenere dati sensibili;

- Perdita o furto di dispositivi: La perdita o il furto di dispositivi come laptop, smartphone o unità di memorizzazione contenenti dati personali può portare a un data breach se tali dispositivi non sono adeguatamente protetti o criptati;

- Errori umani: Gli errori commessi da dipendenti dell'Università o ricercatori, come l'invio di informazioni riservate a destinatari errati o l'accesso non autorizzato a dati da parte di personale interno, possono causare la divulgazione non autorizzata di dati;

Vulnerabilità di sicurezza: Le vulnerabilità nei sistemi informatici o nelle applicazioni possono essere sfruttate da malintenzionati per ottenere accesso non autorizzato ai dati.

FAQ 37. È possibile riutilizzare i dati personali acquisiti, ad esempio, durante una precedente ricerca?

Ai fini della ricerca scientifica o per scopi statistici, l'art. 110 bis del Codice privacy consente di fare istanza al Garante Privacy per chiedere di essere autorizzati al riuso di dati, anche dati personali "particolari", a condizione che siano adottate forme preventive di minimizzazione e di anonimizzazione dei dati ritenute idonee a tutela dei soggetti interessati a fini di ricerca scientifica o per scopi statistici.

Il Garante, laddove autorizza, stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela dei soggetti interessati, che possono essere aggiornate anche successivamente, considerando anche le esigenze di sicurezza. Laddove il Garante non rispondesse entro 45 giorni l'autorizzazione si intende rifiutata.

FAQ 38. Posso svolgere le ricerche a distanza utilizzando piattaforme web?

Si, sempre nel rispetto dei principi etici e delle regole meglio specificate nel progetto depositato prima che sia iniziata la ricerca. Per maggiori approfondimenti si consiglia la lettura delle FAQ 40 e 41.

FAQ 39. Quali sono gli adempimenti minimi in ambito privacy per un corretto svolgimento delle ricerche a distanza?

Il ricercatore, anche nello svolgimento della propria attività di ricerca on line, deve rendere al partecipante un'adeguata informativa sulle tematiche privacy ex art. 13 del GDPR (finalità, basi giuridiche, eventuali destinatari dei dati trattati, tempi di conservazione ecc.) ed acquisire il consenso che costituisce la base giuridica necessaria per intraprendere il trattamento. Il ricercatore dovrà inoltre aver cura di utilizzare una strumentazione hardware e software (telefonica/informatica) adeguata, che rispetti la protezione dei dati e garantisca la privacy dei partecipanti usufruendo di piattaforme sicure che utilizzino quanto meno la cifratura "end-to-end".

FAQ 40. Quali sono gli oneri informativi del ricercatore nello svolgimento della ricerca a distanza?

Nel caso di ricerche con dati personali compiute prevalentemente on line è necessario mantenere traccia e poter dare prova di aver ottenuto il **consenso** e di aver reso al partecipante una **idonea informativa** in merito alle modalità del trattamento dei dati personali acquisiti durante la ricerca (art. 13 Regolamento UE 2016/679).

Occorrerà acquisire il consenso firmato dal partecipante. Un'alternativa potrebbe essere quella di registrare la prima parte dell'incontro con il partecipante alla ricerca fornendogli tutte le informazioni necessarie sul trattamento che verrà effettuato e acquisendo il consenso a detto trattamento – tale registrazione dovrà poi essere conservata dal ricercatore onde poter dimostrare di aver adempiuto agli obblighi di trasparenza previsti dal GDPR e aver ottenuto idonea autorizzazione al trattamento. Il consenso potrà essere ugualmente ottenuto con uno scambio conforme di e-mail.

Nel caso in cui la ricerca con dati personali sia condotta tramite piattaforme web a cui il partecipante accede tramite un account personale riconducibile direttamente alla sua persona, è possibile ottenere il consenso utilizzando una casella posizionata nella pagina web della piattaforma da spuntare con una dichiarazione che potrebbe essere ad esempio "ho letto l'informativa privacy ed acconsento a questo specifico trattamento dei miei dati personali". I partecipanti dovrebbero avere anche la possibilità (in modo semplice e chiaro) di revocare in qualsiasi momento il loro consenso. Se la piattaforma è accessibile anche ai minori potrebbero essere necessari consensi anche da parte dei genitori o dei tutori legali per la raccolta e

l’elaborazione dei dati personali dei minori.

Se i dati sono raccolti in forma anonima non si applica la disciplina del trattamento dei dati personali.

FAQ 41. Quali piattaforme posso usare per effettuare la ricerca a distanza?

Occorre sempre utilizzare una piattaforma web che garantisca elevati livelli di sicurezza. In questo senso è sempre preferibile servirsi delle piattaforme web professionali indicate dall’Ateneo, chiedendo un confronto al Responsabile della protezione dei dati (DPO) dell’Università e/o dell’Ente di ricerca.

FAQ 42. Se i server della piattaforma sono ubicati fuori dall’Italia/Europa, posso utilizzarla lo stesso?

L’aumento delle attività svolte in modalità telematica implica un maggior utilizzo di piattaforme web i cui server sono ubicati all’estero (es. U.S.A. e Australia), configurando sempre più spesso trasferimenti di dati extra UE. A tal proposito, il GDPR stabilisce che i trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo o verso un’organizzazione internazionale sono consentiti a condizione che l’adeguatezza del Paese terzo o dell’organizzazione sia riconosciuta tramite decisione della Commissione Europea (art. 45) ovvero, in assenza di tale decisione, il trasferimento è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46).

Se possibile bisognerebbe prediligere la scelta di gestori che, essendosi adeguati al GDPR, hanno provveduto a stabilire le proprie sedi all’interno del perimetro dell’Unione Europea.

FAQ 43. Come posso provare di aver fornito al partecipante un’adeguata informativa privacy nello svolgimento di una ricerca a distanza?

È necessario poter provare di aver fornito tale documento inviando al partecipante l’informativa sulla privacy, che dovrà essere rispedita sottoscritta, anche con modalità telematiche, al ricercatore.

Tale documento potrà essere ugualmente ottenuto con uno scambio conforme di e-mail.

Nel caso in cui il partecipante non possieda strumenti telematici di trasmissione o nel caso in cui l’indirizzo e-mail fornito dal partecipante non sia a lui immediatamente riconducibile, il ricercatore potrà anche registrare o videoregistrare la sua spiegazione circa le finalità e le modalità adottate per il trattamento dei dati personali, e raccogliere anche un consenso in forma orale, registrato o video-registrato.

APPROFONDIMENTI

Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069677

Codice Etico AIP, https://aipass.org/wp-content/uploads/2023/02/Codice-Etico_luglio-2022.pdf

Regolamento UE 2016/679 (“GDPR”), https://www.garanteprivacy.it/il-testo-del-regolamento

Dichiarazione di Helsinki, https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/