Circolare n. 23 / 2023

Consiglio Nazionale delle Ricerche
Direzione Generale

Ai Direttori/Dirigenti/Responsabili delle Unità Organiche e Strutture del CNR

Personale del CNR

Oggetto: Disciplinare in materia di protezione dei dati personali particolari e relativi a condanne penali e reati del Consiglio Nazionale delle Ricerche in attuazione del Regolamento UE 2016/679.

Nella riunione del 20 giugno 2023, il Consiglio di Amministrazione del CNR ha adottato all'unanimità dei presenti, con deliberazione n. 221/2023, il nuovo Disciplinare in materia di protezione dei dati personali particolari e relativi a condanne penali e reati del Consiglio Nazionale delle Ricerche, di seguito Disciplinare.

Il citato Disciplinare che sostanzialmente abroga il "Regolamento per il trattamento dei dati sensibili e giudiziari del Consiglio Nazionale delle Ricerche" emanato con provvedimento n.18 del Presidente, prot. n. 0002676 del 12 aprile 2007, ha come primario obiettivo l'adeguamento e l'armonizzazione della normativa di cui alla protezione dei dati personali particolari e relativi a condanne penali e reati del Consiglio Nazionale delle Ricerche al Regolamento Europeo n. 2016/679 (RGPD) nonché al Codice in materia dei dati personali di cui al decreto legislativo n.196/2003 (Codice privacy), come modificato dal decreto legislativo 101 del 10 agosto 2018, pubblicato nella G.U. del 4 settembre 2018 ed in vigore dal mese di settembre 2019.

Nell'ambito dell'attuazione del processo di adeguamento e di mantenimento della conformità della normativa interna dell'Ente al RGPD e al Codice privacy, ai fini della stesura del Disciplinare si è reso necessario operare una ricognizione delle attività di trattamento dei dati particolari e relativi a condanne penali e reati con l'obiettivo di dare una chiara ed univoca applicazione in tutto l'Ente dei principi fondamentali del trattamento. Esso rientra all'interno della lista delle attività di "accountability" del titolare e mira a fornire un solido supporto ad una organizzazione territorialmente dislocata su tutto il territorio nazionale al fine di evitare errori materiali di interpretazione della norma. Tale linea di azione, che può essere anche definita quale sorta di linea guida interna, ha una valenza positiva volta ad impedire proprio il disallineamento con la norma come spesso accade nelle attività di trattamento dei dati particolari e relativi a condanne penali e reati.

Si segnalano, in particolare, gli aggiornamenti e/o integrazioni apportati dal Disciplinare, che hanno riguardato i trattamenti relativi a:

- elezione di rappresentanti del personale in seno ad organi politico-amministrativi, di consulenza in accordo con le nuove normative CNR
- gestione delle segnalazioni di Whistelblower introdotte dalla L. 30 novembre 2017, n. 179 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"
- attività di ricerca medica, biomedica ed epidemiologica
- attività di ricerca scientifica nelle scienze tecnico/umanistiche

– attività di servizio di diagnosi e cura anche nell'ambito del Servizio Sanitario Nazionale

Il Disciplinare, inoltre, è stato ampliato con a) l'introduzione delle misure di sicurezza; b) l'introduzione dei tempi di conservazione.

Di seguito un focus sugli elementi innovativi riportati nel Disciplinare in conformità alla normativa europea e nazionale sopra citata, su cui si richiama l'attenzione delle SS.LL.

Misure di sicurezza

La disciplina della protezione dei dati personali è stata oggetto di una riformulazione non formale ma sostanziale che ha cambiato l'approccio stesso alla materia oggi dominata dal principio della responsabilizzazione e dovere di rendicontazione (accountability nel RGPD). Detto principio si sostanzia nell'obbligo per il titolare del trattamento di adottare misure appropriate ed efficaci per attuare i principi di protezione dei dati, nonché nella necessità di dimostrare, su richiesta, che sono state adottate misure tecniche e organizzative appropriate ed efficaci e quindi che il trattamento sia stato effettuato conformemente al RGPD.

Riguardo alle misure di sicurezza, un primo riferimento è contenuto nel disposto dell'art. 22 del GDPR, il quale dispone che il titolare del trattamento dei dati personali debba adottare delle misure tecniche e organizzative idonee al fine di assicurare, ed essere poi in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso.

Più avanti, l'art. 32 del GDPR si occupa nello specifico della sicurezza del trattamento dei dati personali che dovrà essere garantita attraverso l'adozione di una serie di misure concrete adeguate al rischio. In questa valutazione di adeguatezza, il titolare dovrà tenere conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, delle finalità del trattamento, del rischio di probabilità e gravità per i diritti e le libertà degli interessati.

Ad integrare l'approccio di accountability intervengono i principi di privacy by design e privacy by default, sanciti dall'art. 25 del RGPD che richiama i Considerando 75 e 76, i quali impongono l'adozione di misure di protezione fin dalla fase di progettazione del trattamento, oltre a prescrivere un utilizzo dei dati minimo e pertinente, ovvero necessari a rispondere a delle finalità specifiche. Per determinare quali misure adottare, si devono tenere in considerazione anche i rischi e i costi che la loro implementazione comporta. Inoltre, periodicamente devono essere verificate e valutate per assicurarne l'efficacia nel tempo.

In pratica, non esistono più le misure minime di sicurezza, come nella precedente disciplina, ma è il titolare (secondo l'articolazione interna del CNR) che, sulla base del principio di responsabilizzazione, dovrà valutare l'adeguatezza delle misure di sicurezza da mettere in campo, attraverso l'analisi dei rischi ed eventualmente la valutazione d'impatto (art. 35 del RGPD); quest'ultima, in presenza di dati particolari, rappresenta una garanzia per l'applicazione del principio di privacy by design, anche secondo quanto contenuto nelle linee guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248).

Una volta ottemperate tutte le misure organizzative e di sicurezza, i dati possono essere trattati secondo le condizioni di liceità sancite dal RGPD.

Consiglio Nazionale delle Ricerche
Direzione Generale

Nuova definizione di dati particolari

Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali delle persone.

L'art. 22, comma 2, del D.lgs. 101/2018 prevede che le espressioni "dati sensibili" e "dati giudiziari", ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'art. 9 e 10 del Regolamento (UE) 2016/679.

Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.

L'art. 9 del RGDP in linea di principio, prevede che è "vietato trattare 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 ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (art. 9 del GDPR).

Tuttavia, ai sensi del par. 2 dello stesso articolo, sono previste delle deroghe, in virtù delle quali l'Ente può effettuare operazioni di trattamento su categorie particolari di dati personali oltre che a fronte di consenso esplicito prestato dall'interessato, anche per motivi di interesse pubblico rilevante previsti da norma di legge o di regolamento dell'ordinamento europeo o nazionale, che specifichino i dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate, specifiche e proporzionate alla finalità perseguita, per tutelare gli interessi e i diritti fondamentali dell'interessato. La definizione di interesse pubblico rilevante è data all'art. 2-sexies del D.Lgs. 196/2003 (Codice per la protezione dati personali) per il quale "si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri" in varie materie, tra cui (…) l' archiviazione nel pubblico interesse, la ricerca storica (…), la ricerca scientifica (punto cc).

Occorre, in ogni caso, applicare ai trattamenti misure di sicurezza opportune a garantire la minimizzazione dei dati e il rispetto di diritti e libertà per gli interessati, avendo cura di utilizzare la pseudonimizzazione e l'anonimizzazione dei dati, se le finalità da perseguire lo consentono.

A livello nazionale, il nuovo art. 2-septies del D.lgs. 196/2003 richiama l'art. 9 del RGPD, prevedendo che i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni previste dal GDPR, ma stabilisce anche che il trattamento deve avvenire in conformità alle misure di garanzia disposte dal Garante della privacy, misure che, per il momento, non sono state ancora adottate (in particolare, il Garante dovrà precisare le misure di sicurezza da adottare, incluse quelle tecniche di cifratura e di pseudonimizzazione, le misure di minimizzazione, le specifiche modalità di accesso selettivo ai dati, nonché eventuali ulteriori misure volte a garantire i diritti degli interessati).

L'art. 27, comma 1, lett. a), n. 2), del D.lgs. 101/2018 ha abrogato, fra l'altro, l'intero Titolo III del D.lgs. 196/2003; pertanto, anche l'art. 26, che prevedeva che i dati sensibili potevano essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante della privacy, è stato abrogato.

La novella comporta che, allo stato attuale, l'autorizzazione preventiva del Garante non sia più richiesta per il trattamento dei dati indicati all'art. 9 del RGPD (gli ex "dati sensibili"). Con il nuovo regolamento europeo, infatti, l'Autorità di controllo interviene principalmente ex post.

Periodo di conservazione dei dati

Il periodo di conservazione dei dati è un altro degli elementi innovativi che il RGPD ha imposto di indicare, con evidenza, ora nella informativa (art. 13) ora nel registro (art. 30). Con la precisazione che con riferimento alle informazioni di cui all'art. 13 paragrafo 2 lett a) occorre indicare "…il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo".

Come previsto dall'articolo 5, paragrafo 1, lettera e), del RGPD, "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 dovrebbero essere tenuti in considerazione criteri quali la durata e lo scopo della ricerca. Inoltre, l'attività verrà svolta in conformità agli standard metodologici del pertinente settore disciplinare, secondo le specifiche di cui al c. 2, art. 3 delle Regole deontologiche del Garante privacy.

Riuso dei dati per finalità secondarie

Riguardo al riuso dei dati il RGPD amplia i margini per trattare dati personali per finalità secondarie compatibili, come la ricerca scientifica, escludendo il consenso, ad eccezione del caso di riuso dei dati trattati nell'ambito delle sperimentazioni cliniche, e senza autorizzazione preventiva del Garante. (Considerando 33, 50, 159 e Art. 89).

L' Art.110-bis del Codice privacy, restringe i margini per il trattamento e stabilisce che il Garante autorizzi l'uso di dati in conformità all'art. 89 del RGDP comprese forme preventive di minimizzazione e di anonimizzazione dei dati.

Il Regolamento protegge solo le persone fisiche, cosiddetti "interessati" nel momento in cui vengono trattati i loro dati personali. Sono quindi escluse le persone giuridiche, ossia i dati riferiti a quest'ultime. Il regolamento non si applica al trattamento di dati effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico, oppure nel trattamento dei dati effettuati dalle autorità competenti a fini di prevenzione, indagine o accertamento di reati, o per la salvaguardia contro minacce alla sicurezza pubblica.

Coerentemente con le prescrizioni normative previste il CNR ha adottato un modello organizzativo in materia di privacy, in conformità con il proprio assetto ordinamentale (D.lgs 127/2003, D.lgs 213/2009 e D.lgs 218/2016, Statuto 2018 e Regolamento di organizzazione e funzionamento).

A tal proposito si rinvia al provvedimento del Presidente CNR n. 27 del 21 marzo 2019, in materia di Trattamento dei dati personali con il quale sono stati attribuiti i compiti e le funzioni nell'ambito dei trattamenti di competenza ai Responsabili interni al CNR.

Consiglio Nazionale delle Ricerche
Direzione Generale

Per eventuali chiarimenti in merito a quanto previsto dalla presente Circolare è possibile rivolgersi al Gruppo di Lavoro a supporto del Direttore Generale per lo studio e l'approfondimento delle problematiche di tipo giuridico, tecnico ed organizzativo in materia di trattamento dei dati personali nonché per l'elaborazione degli strumenti e delle procedure in applicazione del Regolamento (UE) 2016/679 RGPD al seguente indirizzo e-mail: gdl.privacy@cnr.it .

.

IL DIRETTORE GENERALE
GIUSEPPE COLPANI
06.09.2023 16:57:14
GMT+01:00