SEDE LEGALE
Via Po, 14 - 00198 Roma
T +39 06 47836.1
C.F. 97231970589 ∫ **P.I.** 08183101008
@ crea@pec.crea.gov.it

Circolare n. 4 del 2 luglio 2020

Ai Direttori dei Centri di Ricerca
Loro Sedi

Ai Dirigenti amministrativi
Loro Sedi

Oggetto: Gestione del trattamento dati ai sensi del Reg. UE n. 679/2016 (GDPR) e del decreto legislativo n. 196/2003 ("Codice in materia di protezione dei dati personali"), come modificato dal decreto legislativo n. 101/2018.

Allo scopo di consentire la corretta applicazione delle prescrizioni contenute nel Regolamento (UE) 2016/679 del 27 aprile 2016 (GDPR – *General Data Protection Regolation*) e nel decreto legislativo 30 giugno 2003, n. 196, (Codice in materia di protezione dei dati personali), come modificato dal decreto legislativo 10 agosto 2018, n. 101, si ritiene opportuno fornire una serie di indicazioni operative di cui tener conto nell'espletamento delle variegate attività dell'Ente.
A tal riguardo, è necessario individuare le figure deputate o comunque interessate alla gestione dei dati personali, nonché i rispettivi adempimenti e responsabilità. Si può trattare sia di figure interne all'organizzazione amministrativa, sia di soggetti esterni che, entrando in contatto con l'Amministrazione, possono trovarsi nella condizione di dover gestire dati personali.

Oggetto del trattamento.
In via preliminare, tuttavia, è opportuno partire dall'oggetto del trattamento, ovvero dalla definizione di **dati personali**.
Sono dati personali tutte quelle informazioni che riguardano una persona fisica identificata o identificabile, definita "**interessato**".
Il Garante per la protezione dei dati personali (in seguito "Garante") pone l'accento su dati di particolare rilievo, quali:
• i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

• i dati rientranti in particolari categorie: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, nonché i dati relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679

(articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;

• i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie hanno assunto un ruolo significativo anche altre tipologie di dati, quali quelle relative alle comunicazioni elettroniche (tramite rete Internet o linee telefoniche) e quelle che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Soggetti del trattamento.
È ora opportuno identificare **le figure soggettive** interessate al trattamento dei dati personali, con particolare riferimento a quelle **interne all'Amministrazione**.

Titolare del trattamento.
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 e i mezzi del trattamento dei dati personali.
Con diversi pronunciamenti il Garante ha più volte chiarito che per quanto riguarda gli Organismi pubblici (tra i quali rientra il CREA), il titolare del trattamento è l'Ente nella sua interezza ancorché rappresentato all'esterno da un Presidente o da una figura investita di analoghi poteri (ad esempio da un Commissario ove l'Ente si trovi in gestione commissariale).
Le attività demandate al titolare del trattamento non hanno natura gestionale ma si sostanziano nella potestà di decidere il motivo e le modalità del trattamento. In ragione di ciò il titolare del trattamento è chiamato ad adottare un modello organizzativo in cui vengono formalmente individuati tutti i soggetti che, a vario titolo, entrano nel processo di gestione dei dati, caratterizzandolo e determinandolo.
Il titolare del trattamento è giuridicamente responsabile dell'ottemperanza degli obblighi imposti dalla normativa vigente in tema di protezione dei dati personali, sia a livello nazionale che internazionale, compreso l'obbligo di notifica al Garante nei casi previsti.

I soggetti delegati attuatori (Responsabili interni del trattamento).
Il decreto legislativo 10 agosto 2018, n. 101, emanato per armonizzare le disposizioni nazionali con quelle comunitarie, ha tenuto conto della necessità di attribuire l'effettiva gestione dei dati agli Uffici o ai Servizi interessati ed ha a tal fine previsto le figure dei soggetti delegati attuatori.
Esse coincidono con i Dirigenti dei Servizi che, per le loro attività, gestiscono dati personali.
Nell'organizzazione del CREA sono soggetti delegati attuatori i Dirigenti, per l'amministrazione centrale, e i Direttori per i Centri di ricerca con riferimento alla articolazione periferica.

Detti soggetti avranno, in particolare, il compito di:
- verificare la legittimità dei trattamenti;
- adottare nell'ambito dei procedimenti di interesse le soluzioni definite "privacy by design" e "privacy by default";
- tenere costantemente aggiornato il registro delle attività del trattamento;
- fornire istruzioni ai soggetti autorizzati ("incaricati del trattamento");
- predisporre ogni adempimento organizzativo necessario.

Gli incaricati del trattamento.
Sono i soggetti materialmente incaricati del trattamento in ragione dell'attività specificamente svolta (ad esempio le procedure di gara a supporto del RUP).
Sono formalmente incaricati dal soggetto delegato attuatore che dovrà impartire tutte le necessarie istruzioni per l'espletamento delle attività legate al trattamento dei dati.

Soggetti esterni in rapporti contrattuali o convenzionali con l'Ente.
Non tutti i rapporti contrattuali generano l'acquisizione e la conseguente gestione di dati personali. Tuttavia, ogni ciò dovesse verificarsi, è necessario adottare specifiche misure che sono essenziali per il rispetto delle disposizioni normative e per la validità stessa dei rapporti contrattuali/convenzionali.
Di seguito vengono esaminate le situazioni ricorrenti, ovvero:

1) Quando vi è contitolarità della gestione dei dati;
2) Quando, ferma restando la titolarità, si alloca la responsabilità della gestione ad un soggetto esterno all'Amministrazione.

1) La contitolarità (art. 4, n. 7 e art. 26 del DGPR).
Due soggetti possono assumere la qualifica di contitolari quando, rispetto ad uno o più trattamenti, determinano congiuntamente finalità e mezzi del trattamento.
Si riportano di seguito alcune ipotesi a titolo meramente esemplificativo:
a) Il CREA e un'altra pubblica amministrazione si accordano (con un protocollo, una convenzione o con un atto giuridico analogo) per svolgere una determinata attività o un progetto che comporta il trattamento di dati personali, ed entrambi i soggetti possono essere competenti a trattare i dati relativi in ragione della tipologia di attività svolta ovvero in ragione del tipo di accordo, contratto o convenzione;
b) Il CREA è chiamato ad assumere un ruolo di garanzia e/o di controllo su una determinata attività o tematica che viene posta in essere a seguito di convenzioni, protocolli o intese sottoscritti con altri soggetti pubblici o privati;
c) Il CREA realizza un partenariato con altri enti (pubblici o privati) per la partecipazione a programmi o progetti per il finanziamento di determinate attività che possono comportare l'acquisizione e la gestione di dati personali;
d) Il CREA in ragione di previsioni normative o di specificità riguardanti la sua missione istituzionale pone in essere progetti o servizi che vanno gestiti con altri enti similari.
In ipotesi quali quelle sopra individuate è necessario che, sin dall'inizio delle interlocuzioni, il soggetto proponente verifichi con la controparte contrattuale se si possono realizzare casi di in cui i

dati di ciascuno saranno messi in comune, pur senza cessione degli stessi, ovvero se esista una possibile contitolarità dei dati.
In tale ipotesi, le parti potranno:

a) inserire già nell'atto la definizione delle responsabilità in capo a ciascuno;
b) sottoscrivere un accordo separato che elenchi gli obblighi e le responsabilità di ciascuno in relazione alla condivisione dei dati.

In caso di contitolarità potrà essere indicato anche un unico soggetto che, per entrambi i contraenti, si preoccupi di rilasciare l'informativa agli interessati, di raccogliere i consensi e di individuare il soggetto che si interfaccia con gli interessati in caso di esercizio dei relativi diritti.
Si potrà essere contitolari anche nel caso in cui si tratti di una raccolta di nuovi dati mai gestiti dalle parti e per i quali andrà effettuato un nuovo trattamento, oppure nel caso in cui si trattino dati già posseduti utilizzando delle nuove tecnologie. In questo caso va verificato se esistano dei rischi per gli interessati e le misure da adottare per il contenimento degli stessi.
Altro caso potrà essere quello in cui le parti dovranno sviluppare degli applicativi informativi, dei portali informativi e gestionali o strumenti similari. In questo caso le responsabilità vanno definite anche per le fasi di progettazione, in ossequio al principio della privacy by design, individuando le misure di sicurezza adottate per la tutela dei dati ovvero la privacy by default, e chi sia il responsabile che si occuperà di gestire questo processo.
Si allega a tal fine uno schema contrattuale per il caso della contitolarità.

2) Responsabili esterni del trattamento.
Quando l'Ente si trova ad esternalizzare o ad acquisire un servizio, può accadere che il soggetto incaricato debba accedere a dati personali per espletarlo.
In questo caso l'Ente, in qualità di titolare del trattamento, deve provvedere ad adempiere alle disposizioni di cui all'articolo 28 del GDPR.
In particolare, il titolare del trattamento nomina con un contratto o altro atto giuridico idoneo il responsabile del trattamento e gli fornisce le istruzioni necessarie per la corretta gestione del dato, chiedendogli di attestare e, nei casi più complessi, di certificare la sua capacità di porre in essere tutte le misure necessarie alla tutela della privacy.
Quando si va ad esternalizzare un servizio, già nel capitolato di gara vanno previste ed indicate le caratteristiche che l'aspirante contraente deve possedere al fine di assicurare la corretta gestione dei dati.
All'atto della stipula del contratto, un apposito allegato dovrà disciplinare gli obblighi gravanti sul contraente selezionato in qualità di responsabile del trattamento.

Misure: Privacy by design e privacy by default.
Il Regolamento UE per la protezione dei dati personali prevede un approccio basato sulla prevenzione del rischio e pertanto introduce all'art. 25 il principio di "privacy by design" e di "privacy by default", ovvero l'obbligo di prevedere da subito, in un progetto basato sull'utilizzo di tecnologie informatiche, quali siano gli strumenti e le corrette impostazioni del sistema per la tutela dei dati personali e quali siano le attività previste a conclusione del ciclo di gestione.
Va assicurato che i dati vengano gestiti solo per le attività di interesse e per il tempo strettamente necessario; vanno assicurati i principi di sicurezza, visibilità e trasparenza dei trattamenti nonché le modalità per fornire una celere risposta agli utenti in caso di accesso.

Nel caso in cui si utilizzino software ed applicativi di terzi, sarà compito e cura del fornitore effettuare e certificare queste operazioni.

La sicurezza informatica e l'amministratore di sistema.

Nel sistema di sicurezza per la gestione informatica dei dati, una figura di rilievo è quella dell'amministratore di sistema che il Garante definisce: "*una figura professionale dedicata alla gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali , compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza nella misura in cui consentano di intervenire sui dati personali"* (Provvedimento 27.11.2008).

Si tratta di un incarico prettamente tecnico che, tuttavia, ha un impatto significativo in termini di responsabilità sui dati "aziendali".

Il Regolamento comunitario non prevede espressamente la figura di amministratore di sistema. Tuttavia, un richiamo implicito può essere rinvenuto all'articolo 32 del GDPR ove si stabilisce che il titolare del trattamento ed i responsabili interni del trattamento devono mettere in atto delle misure tecniche per garantire un adeguato sistema di protezione dei dati e, quindi, un livello di sicurezza adeguato al rischio.

Le procedure descritte nel richiamato art. 32 del GDPR hanno una valenza prettamente tecnica e riguardano, ad esempio, la cifratura dei dati, il loro ripristino in caso di incidenti fisici o tecnici nonché le necessarie verifiche periodiche delle misure adottate e, pertanto, richiedono l'intervento di figure tecniche esperte sotto l'aspetto informatico.

Il legislatore europeo dispone poi un nucleo minimo di misure che rispondono a criteri di sicurezza predefiniti. Tra esse sono comprese:

- la pseudonimizzazione e 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;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Per quanto sopra descritto l'amministratore di sistema diventa una figura professionale rilevante ed essenziale per garantire la sicurezza delle banche dati, per svolgere funzioni molto delicate che implicano la reale possibilità di accedere a tutti i dati che transitano sulla rete aziendale, nonché per la necessità di vigilare sul corretto utilizzo delle attrezzature informatiche dell'Ente. L'amministratore di sistema, proprio grazie alla sua attività continua, dovrebbe essere il primo ad accorgersi se si sia verificata una perdita o una violazione dei dati (cosiddetto "data breach"). Colui o coloro che sono chiamati a svolgere la funzione di amministratore di sistema devono essere persone di esperienza, con rilevanti capacità professionali atte a garantire il pieno rispetto della normativa di settore.

Allegati alla presente circolare esplicativa si forniscono fac simili utilizzabili con eventuali adattamenti.

Antonio Di Monte
Direttore Generale f.f.

In allegato:
Format per la contitolarità dei dati (Allegato 1)
Format per l'indicazione del responsabile del trattamento direttamente in contratto (Allegato 2)
Format da allegare al contratto (Allegato 3)
Format per la nomina di responsabile esterno del trattamento (Allegato 4)