DISCIPLINARE
MODELLO ORGANIZZATIVO
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Approvato con Decreto Commissariale n…75…del…15.06.2020.

INDICE

Considerazioni generali

CONSIDERAZIONI GENERALI

Il Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione dei dati personali delle persone fisiche con riguardo al trattamento di tali dati ed alla libera circolazione degli stessi (di seguito anche solo “Regolamento”) disegna una complessa articolazione operativa, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni.

Le disposizioni del D.lgs. 196/2003 “Codice in materia di protezione dei dati personali”, per come modificato dal D.lgs n. 101/2018, nonché i Provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito anche solo “Garante”), continuano a trovare applicazione ove non siano in contrasto con la normativa succitata.

Per dare attuazione ai suddetti obblighi ed adempimenti, e tenuto conto della specifica ed articolata organizzazione del CREA, occorre rivedere l’assetto relativo alla definizione e distribuzione delle responsabilità in capo a ciascuno dei soggetti previsti dal Regolamento UE.

Il suddetto Regolamento europeo individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

● il titolare del trattamento: 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 di dati personali;

● il responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Il Responsabile interno del trattamento è il soggetto delegato attuatore.

● il Responsabile della protezione dei dati (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;

● gli incaricati del trattamento sono le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di “terzo” di cui al n. 10 del comma 1 art. 4 del Regolamento.

Tutte le figure sopra indicate danno vita ad una organizzazione di tipo piramidale che, tuttavia, è chiamata a governare un processo circolare nel quale il dato viene identificato, gestito, conservato e successivamente eliminato secondo regole precise e, soprattutto, con le garanzie dovute al soggetto cui il dato appartiene e che è l’interessato. L’interessato deve poter conoscere il ciclo della gestione, chi siano i soggetti che vi partecipano con i loro adempimenti e quali siano le garanzie offerte affinché i suoi dati siano tutelati.

Con il presente disciplinare il CREA definisce il proprio ambito di titolarità, le attribuzioni in capo ai soggetti delegati attuatori Responsabili del Trattamento, indica i compiti assegnati al DPO designato e definisce i criteri generali da rispettare nell'individuazione dei soggetti autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito delle responsabilità, come sintetizzato nello schema di seguito riportato.

1. Il titolare

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4, n. 7, e dell'art. 24 del Regolamento, è il CREA nella persona del rappresentante legale cui spetta l'adozione di misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al Regolamento. Spetta pertanto in particolare al titolare:

● adottare il modello organizzativo conformemente alle disposizioni normative e con riferimento alle previsioni del Codice per la protezione dei dati personali;

● designare il Responsabile della protezione dei dati;

● designare i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;

● effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il DPO designato;

● istruire i soggetti autorizzati al trattamento dei dati personali.

2. I Soggetti delegati attuatori / Responsabili interni del Trattamento

Sono designati quali soggetti delegati attuatori degli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dal CREA:
i Dirigenti dell'Amministrazione Centrale, ciascuno per i propri ambiti e competenze;
i Direttori dei centri di ricerca.

Di seguito, sono indicati i compiti affidati ai soggetti delegati attuatori:

A) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;

B) disporre, in conseguenza alla verifica di cui alla lett. A), le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;

C) adottare soluzioni di privacy by design e by default;

D) tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;

E) predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento;

F) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;

G) predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;

H) provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;

I) disporre l'adozione dei provvedimenti imposti dal Garante;

J) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

K) adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri Soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;

L) individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;

M) garantire al Responsabile del Servizio competente in materia di sistemi informativi e al DPO i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

N) effettuare preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

O) consultare il Garante, in aderenza all'art. 36 del Regolamento e nelle modalità previste dal par. 3.1, lett. b), nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;

P) richiamare obbligatoriamente nei contratti di sviluppo di software e piattaforme, la policy in materia di sviluppo delle applicazioni, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del contratto;

Q) designare gli incaricati del trattamento.

Nell'attuazione dei compiti sopraindicati i soggetti delegati possono acquisire il parere del DPO nei casi e con le modalità specificate nel seguito.

3. I Responsabili esterni del Trattamento

Sono designati responsabili del trattamento di dati personali i soggetti esterni all'Ente che siano tenuti, a seguito di convenzione, accordo, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare.

Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni o accordi e, in ogni caso, in costanza di formazione del rapporto contrattuale.

4. Gli incaricati

Sono i tutti i soggetti che effettuino operazioni di trattamento, dipendenti e collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare o dei soggetti delegati.
Tali soggetti devono essere da questi formalmente autorizzati tramite:

- individuazione nominativa (nome e cognome) delle persone fisiche. In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare;
- tramite assegnazione funzionale della persona fisica al Servizio, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale Servizio.

La designazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento.
Tali istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo al rispetto delle regole di riservatezza in caso di mobilità interna nonché le regole dettate dall'Ente in materia di sicurezza informatica e protezione dei dati personali.

5. Il Responsabile della Protezione dei dati (DPO) – Pareri del DPO

Il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO).

Specificatamente, sono di seguito indicati i compiti del DPO in aderenza agli articoli 37 e ss. del suddetto Regolamento, conformati alla precipua organizzazione dell'Azienda:

- informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con il supporto dei Responsabili interni del Trattamento e con il supporto del gruppo dei referenti designati;
- vigila sull'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Ente in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- coopera con il Garante per la protezione dei dati personali;
- funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del Sistema Informativo o ne richiede di specifiche;
- promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;
- partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy di Ente;
- formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento;
- fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato di seguito.

Pareri del DPO
Il DPO fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture dell'Ente presentano nei casi di seguito indicati.

6. Pareri obbligatori /Pareri facoltativi

Pareri obbligatori

Devono essere obbligatoriamente richiesti pareri in ordine a:

● individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'Ente intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo anche a seguito di incidenti di sicurezza o analisi dei rischi;

● adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;

● individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;

● incidenti sicurezza.

Pareri facoltativi

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:

● progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;

● valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento 2016/679;

● valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016;

● opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Le richieste di parere devono essere inviate all'indirizzo di posta elettronica del Servizio di assegnazione del DPO nelle modalità che saranno stabilite dall' Ente.

Possono presentare le richieste di parere i dirigenti e i Direttori quali soggetti delegati attuatori e, pertanto responsabili interni del trattamento dati personali.

I pareri sono espressi nel rispetto delle seguenti codifiche:

1. ● NC: acronimo di "non conformità", nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;
2. ● OS: acronimo di "osservazione", nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;
3. ● PO: acronimo di "positivo", nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy regionali in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima pareri "NC" e "OS" il soggetto delegato attuatore deve formalizzare, nelle medesime forme utilizzate dal DPO per l'espressione del parere, le motivazioni che giustificano l'esecuzione dell'attività o l'implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal DPO.

I pareri espressi dal DPO sono conservati agli atti del soggetto delegato.

7. Il Servizio Informativo dell'Ente

Il Servizio competente in materia di sistemi informativi, ovvero di sicurezza informatica, svolge un ruolo di supporto al DPO in tema di risorse strumentali e di competenze.

Nell'ambito dell'Ufficio addetto ai sistemi informativi, ovvero associato ad esso in forma di collaborazione, è individuato **l'amministratore di sistema** con funzione di supporto tecnico e di coordinamento delle attività finalizzate a garantire la sicurezza informatica.

Il Servizio informativo:

● individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo del CREA. Tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo obbligatorio del DPO, come ad esempio per la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e per la redazione ed aggiornamento dei disciplinari tecnici trasversali;

● condivide le evidenze dell'analisi dei rischi con il DPO, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;

● provvede, ogni qualvolta venga avvertito un problema di sicurezza a:

○ attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del DPO;

○ individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO;

○ segnalare al Titolare/Responsabile del Trattamento le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali;

● svolge verifiche sulla puntuale osservanza della normativa e delle policy in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del DPO e realizza le verifiche specifiche richieste dello stesso;

● promuove la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all'interno dell'Ente, coordinandosi con le azioni promosse dal DPO.

8. Il Gruppo dei referenti privacy

Costituisce attuazione dei principi di informazione e sensibilizzazione del Regolamento europeo n. 679/2016 la costituzione di un gruppo permanente di referenti privacy che assicuri un presidio per le strutture dell'Ente per quel che concernono gli adempimenti continuativi, lo studio e l'approfondimento degli aspetti

normativi, organizzativi e procedurali, derivanti anche delle nuove disposizioni normative.
Il Gruppo di referenti ha i seguenti compiti:

- effettuare la ricognizione costante, a mezzo del Registro, dei trattamenti di dati personali effettuati dalle strutture di appartenenza, servendosi di risorse e competenze messe all'uopo a disposizione dal soggetto delegato attuatore o dal soggetto dallo stesso delegato;
- fornire supporto alle verifiche di sicurezza svolte dal Servizio ICT e/o dal DPO;
- provvedere alla revisione e all'aggiornamento dei Disciplinari Tecnici;
- coordinare le richieste di parere al DPO dei soggetti delegati attuatori di propria afferenza nei casi e con le modalità previsti dal presente documento.

9. Rinvio

Per quanto non previsto dal presente disciplinare si rinvia a specifici atti successivi, ovvero a circolari esplicative e/o protocolli operativi.