Canale Emiliano Romagnolo

MODELLO ORGANIZZATIVO

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

adottato con delibera n.639/18/DA in data 28/09/2018

Sommario

1. Indirizzi generali

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito anche solo "Regolamento") detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, 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", nonché i Provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante"), continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa succitata. Si evidenzia che è previsto comunque l'adeguamento della normativa nazionale alle disposizioni del Regolamento.
Per dare attuazione ai suddetti obblighi ed adempimenti, occorre rivedere l'assetto delle responsabilità tenuto conto della specifica organizzazione del Consorzio di bonifica per il Canale Emiliano Romagnolo (CER).
Il 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 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;
- 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.

Con il presente documento il CER definisce il proprio ambito di titolarità, delega al Direttore generale e ai Direttori di Area l'attuazione degli adempimenti previsti dalla normativa, 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.

2. Il titolare

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

- adottare, nelle forme previste dal proprio ordinamento, gli interventi normativi necessari, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali oggetto di prossimo adeguamento al Regolamento;
- designare il Responsabile della protezione dei dati (DPO);
- 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;
- adottare le policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario; coadiuvato dal gruppo per la gestione della Sicurezza ICT e dagli Amministratori di Sistema
- sottoscrivere gli atti di notifica e di consultazione preventiva al Garante, attività che può essere delegata al Direttore generale;
- notificare e la comunicare le violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento, attività che può essere delegata al Direttore generale;
- dispone l'adozione dei provvedimenti imposti dal Garante;
- designare i Responsabili esterni del trattamento.

3. I Soggetti delegati attuatori

Sono designati quali soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dal CER in esecuzione del regolamento:

- Il Direttore generale
- Il Direttore dell'Area Amministrativa - *in ragione dei compiti affidati*
- Il Direttore dell'Area Tecnica – *in ragione dei compiti affidati*
- Il Direttore dell'Area Agronomico-ambientale - *in ragione dei compiti affidati*

Relativamente ai trattamenti di dati personali trasversali a più strutture si applica il criterio della prevalenza.

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 *(tutti i soggetti attuatori);*
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 *(tutti i soggetti attuatori);*
C. adottare soluzioni di privacy by design e by default (*tutti i soggetti attuatori);*
D. dare informazioni utili agli uffici per tenere aggiornato il registro delle attività di trattamento per la struttura di competenza *(Direttore generale e Direttore dell'Area Amministrativa);*
E. predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento da sottoporre alla firma del titolare del trattamento;
F. supportare il titolare nell'individuazione 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; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
G. predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa *(tutti i soggetti attuatori);*
H. provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa *(Direttore generale);*
I. collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate *(tutti i soggetti attuatori)*;
J. adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri 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 *(tutti i soggetti attuatori);*
K. 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 *(tutti i soggetti attuatori);*
L. garantire al Servizio informatico 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 *(tutti i soggetti attuatori);*

M. 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 *(tutti i soggetti attuatori);*

N. 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 *(Direttore generale);*

O. 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 *(tutti i soggetti attuatori).*

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

Fermo restando che la responsabilità delle attività sopraindicate rimane in ogni caso in capo al soggetto delegato attuatore, in ragione del fatto che non sono ascrivibili a funzioni di direzione, coordinamento generale e controllo, in base ai principi generali relativi all'istituto della delega, sono eventualmente subdelegabili i compiti di cui alle lettere *d), e), f)*

Tali compiti sono delegabili:

- Capi Settore, Capi sezione o Collaboratori Direttivi e Unità di Staff

4. Gli amministratori di sistema

Per o svolgimento delle mansioni di amministratori di sistema il CER si avvale di collaborazioni con altri enti associati ovvero di prestazioni professionali reperite sul mercato.

Gli amministratori di sistema adottano tutte le misure necessarie per proteggere gli elaboratori dalle infezioni da virus informatici o da accessi al sistema non autorizzati.

Adottano le modalità di creazione e la periodicità delle copie di back up dei dati trattai per mezzo degli elaboratori a lei affidati, nonché la conservazione in luogo sicuro dei supporti removibili utilizzati per memorizzare tali copie.

Adottano le modalità tecniche di sistema di ripristino dei dati in caso di accidentale distruzione o alterazione.

Adottano le modalità di distruzione dei supporti removibili non più utilizzati nei quali sono state memorizzate le copie di back up contenenti dati sensibili o giudiziari.

Adottano le modalità di riutilizzo dei supporti removibili non più utilizzati nei quali sono state memorizzate le copie di back up contenenti dati sensibili in modo tale che i dati precedentemente memorizzati non siano in alcun modo ricostruibili.

Assegnano le credenziali di autenticazione ad ogni incaricato avendo cura di non riutilizzare le stesse credenziali per altri incaricati, anche in tempi diversi.

Provvedono alla disattivazione delle credenziali in caso di mancato utilizzo per oltre sei mesi o in caso di revoca di incarichi assegnati.

Comunicano ad ogni incaricato del trattamento dei dati le credenziali di accesso e le password provvisorie.

Valutano periodicamente l'efficienza delle misure di sicurezza adottate in base all'innovazione tecnologica.

Istruiscono adeguatamente il personale incaricato al trattamento dei dati sull'utilizzo degli strumenti informatici, sia hardware che software, affinché non venga mai pregiudicata la sicurezza dei dati o delle copie di sicurezza.

Organizzano i flussi di rete. Manutengono l'hardware. Adottano sistemi idonei alla registrazione degli accessi logici degli amministratori di sistema. Le registrazioni devono contenere il riferimento temporale a 1 evento e devono essere persistenti per un minimo di sei mesi.

Comunicano tempestivamente al responsabile del trattamento o al titolare qualsiasi circostanza che possa pregiudicare il trattamento dei dati o la loro sicurezza.

5. Gruppo per la Gestione della sicurezza ICT

E' formato da un responsabile per la gestione della sicurezza ICT, un referente per la gestione della sicurezza informatica, un componente esperto del servizio informatico competente. Il gruppo sarà coadiuvato da altre figure professionali reperite all'interno dell'amministrazione ed individuate dalle Direzione Generale con specifici atti di organizzazione, con le seguenti competenze:

- rappresentare il punto di riferimento univoco a cui il personale dell'organizzazione deve rivolgersi per segnalare un potenziale incidente oppure un comportamento sospetto;
- gestire tutte le attività inerenti l'analisi e la gestione di un incidente di sicurezza, ivi comprese quelle relative alla sua notifica e documentazione;
- garantire la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori), necessarie per la gestione di un incidente di sicurezza;
- garantire che il processo di gestione incidenti sia sempre adeguato alle esigenze dell'ente, provvedendo che sia sempre aggiornato.

I riferimenti del gruppo (nominativi, indirizzo e-mail, numero di telefono ecc.) devono essere ben identificati e facilmente raggiungibili.

Il gruppo deve includere un referente per la gestione della sicurezza informatica che avrà il compito di supportare il gruppo e il responsabile nella gestione degli incidenti svolgendo le necessarie funzioni di raccordo con la struttura e con il servizio informatico competente.

Nel corso del processo di gestione di un incidente di sicurezza informatico e, eventualmente, di un data breach, il gruppo potrà essere coadiuvato di volta in volta dal personale della struttura i cui dati sono stati oggetto di data breach e da tutti coloro che il gruppo riterrà necessario coinvolgere a seconda della tipologia di incidente e della tipologia di dati coinvolti.

Nelle attività del gruppo deve essere coinvolto il Data Protection Officer (DPO) designato, il quale esercita le proprie funzioni di monitoraggio della conformità in caso di data breach, fornendo il proprio parere in ordine alla necessità di effettuare la notifica e, quindi, sulle valutazioni precedentemente descritte.

6. Il Responsabile per la gestione della sicurezza ICT

Il Responsabile per la gestione della sicurezza ICT che ha il compito di attivare il gruppo in caso di incidenti di sicurezza, di individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO, e di segnalare al Direttore Generale le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali. La notifica è effettuata a cura del Direttore o, in sua assenza, da un dirigente di area.

Il Responsabile deve inoltre coinvolgere, a seconda della gravità dell'incidente, i direttori di area del Consorzio per gli aspetti di comunicazione interna ed esterna e nel caso, durante la gestione dell'incidente, emergano responsabilità da parte di personale interno dell'Ente occorre coinvolgere la struttura che si occupa di gestione del personale.

Nel caso in cui le attività di analisi dell'incidente di sicurezza evidenzino particolari difficoltà oppure impatti che si estendono al di fuori del perimetro dell'Ente, il Responsabile deve valutare l'opportunità o la necessità, di coinvolgere le strutture di riferimento regionali e nazionali (ad esempio Lepida SpA considerando il proprio ruolo nell'ambito della sicurezza della Community Network, CERT-PA, …). Inoltre, il Responsabile deve prevedere il coinvolgimento dei propri fornitori di servizi ICT e del servizio informatico competente per il supporto all'analisi e per l'ottenimento di informazioni utili oltre alle autorità di pubblica sicurezza nel caso in cui l'incidente possa presentare risvolti dal punto di vista penale.

In caso di assenza del Responsabile subentra il referente, che è tenuto ad informare puntualmente il direttore dell'Area amministrativa e il Responsabile della comunicazione.

7. Il Servizio informatico competente

Il servizio informatico competente è il fornitore o il soggetto che eroga i servizi informatici in forza di apposito contratto provvede all'organizzazione e supervisione di tutte le attività informatiche del Consorzio e fornisce supporto tecnico specialistico nella gestione degli incidenti di sicurezza.

In caso di data breach il punto di contatto con il Garante per la protezione dei dati personali è costituito dal Data protection officer.

Il CER conforma la propria attività di trattamento e gestione dei dati anche mediante l'adozione di regolamenti finalizzati alla prevenzione degli incidenti di sicurezza, riducendo il livello di rischio e l'esposizione a possibili attacchi informatici. Tali contromisure, che possono essere di natura sia tecnologica che organizzativa, devono essere descritte e adottate dal Consorzio per mettere in sicurezza i sistemi ICT, avvalendosi del supporto del/dei fornitori di servizi ICT e del servizio informatico competente.

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. E' cogestito per il quinquennio 2017 - 2021 con convenzione in data 6 novembre 2017 con Consorzio di bonifica della Romagna, ente dotato di personale qualificato in materia informatica, associato al CER.

Il sistema informatico condiviso fa capo ai Datacenter Lepida di Ravenna

Al fine di adeguare le funzioni assegnate con la designazione della nuova figura del DPO è necessario prevedere per il Servizio DPO i compiti di seguito meglio specificati:

- individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente. 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 Direttore Generale competente in materia di sistemi informativi 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 regionali 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 del CER, coordinandosi con le azioni promosse dal DPO.

8. I responsabili del trattamento

Sono designati responsabili del trattamento di dati personali i soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, 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 e, in ogni caso, in costanza di formazione del rapporto contrattuale, in aderenza ai fac-simili messi a disposizione dalla struttura competente in materia di privacy.

9. Gli incaricati

Sono autorizzati al compimento alle operazioni di trattamento dei dati i soggetti delegati attuatori di cui al precedente paragrafo ed i dirigenti da loro delegati ai sensi della presente disciplina, che conformano i loro trattamenti alle policy regionali in materia di protezione dei dati personali e alle istruzioni di seguito riportate:

- sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- sono verificati legittimità e correttezza dei trattamenti, verificando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Sono, altresì, autorizzati 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.

Gli incaricati sono quindi designati:

- 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 alla unità organizzativa di minori dimensioni, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.

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 alle policy del CER in materia di sicurezza informatica e protezione dei dati personali.

10. Il Responsabile della Protezione dei Dati (DPO/RPD)

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, o Responsabile Protezione Dati di seguito DPO).

Specificatamente, sono di seguito indicati i compiti del DPO in aderenza agli 37 e ss del suddetto regolamento, conformati alla precipua organizzazione del CER:

- informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con il supporto del gruppo dei referenti designati dalle strutture;
- sorveglia l'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 servizio ICT competente 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 dell'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.

11. 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.

12. 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 dell'Ente, 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.

13. 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 cer@consorziocer.it nelle modalità che saranno stabilite dall'Ente.

Possono presentare le richieste di parere i soggetti delegati attuatori o i dirigenti delegati in base ai principi generali relativi all'istituto della delega.

I pareri sono espressi nel rispetto delle seguenti codifiche:

- 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;

- 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;
- 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.

14. 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:

- attuare, per le strutture di appartenenza, le misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall’Ente, anche a seguito di analisi ed approfondimenti in seno al Gruppo dei referenti privacy;
- coordinare il puntuale aggiornamento delle designazioni degli amministratori di sistema all’interno delle Direzioni/strutture di appartenenza e la costante verifica dei privilegi assegnati agli amministratori già designati;
- 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 dirigente 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.

15. Accesso civico generalizzato e ruolo DPO

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il DPO, le strutture dell'Ente, e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.).

Il D.L. 97/2016, di modifica del D.lgs. 33/2013 ha introdotto l'istituto dell'accesso civico "generalizzato", che attribuisce a "chiunque" il "diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione.

L'esercizio di tale diritto soggiace ai limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis" del d.lgs. n. 33/2013).

L'art. 5, c. 5, d.lgs. n. 33/2013 prevede che, per ciascuna domanda di accesso generalizzato, l'amministrazione debba verificare l'eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria.

Il DPO funge da supporto alle strutture competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato.

Il DPO funge altresì da supporto al R.P.C.T. nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali.

Il DPO, inoltre, su richiesta delle strutture, esprime proprio parere in ordine alla valutazione dell'eventuale pregiudizio che l'accesso 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.

Il DPO, su richiesta delle strutture, formula il proprio parere, entro tre giorni, in ordine all'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.

Sulla scorta di tale parere le strutture competenti sulle singole richieste di accesso effettueranno il bilanciamento tra gli interessi asseritamente lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.