# REGIONE EMILIA-ROMAGNA
## Atti amministrativi
## GIUNTA REGIONALE

Delibera Num. 1123 del 16/07/2018

Seduta Num. 31

**Questo** lunedì 16 **del mese di** luglio

**dell' anno** 2018 **si è riunita nella residenza di** via Aldo Moro, 52 BOLOGNA

**la Giunta regionale con l'intervento dei Signori:**

| | |
|---|---|
| 1) Bonaccini Stefano | Presidente |
| 2) Gualmini Elisabetta | Vicepresidente |
| 3) Bianchi Patrizio | Assessore |
| 4) Caselli Simona | Assessore |
| 5) Corsini Andrea | Assessore |
| 6) Donini Raffaele | Assessore |
| 7) Petitti Emma | Assessore |
| 8) Venturi Sergio | Assessore |

**Funge da Segretario l'Assessore:** Bianchi Patrizio

**Proposta:** GPG/2018/1131 del 29/06/2018

**Struttura proponente:** SERVIZIO ICT REGIONALE
DIREZIONE GENERALE RISORSE, EUROPA, INNOVAZIONE E ISTITUZIONI

**Assessorato proponente:** ASSESSORE AI TRASPORTI, RETI INFRASTRUTTURE MATERIALI E IMMATERIALI, PROGRAMMAZIONE TERRITORIALE E AGENDA DIGITALE

**Oggetto:** ATTUAZIONE REGOLAMENTO (UE) 2016/679: DEFINIZIONE DI COMPETENZE E RESPONSABILITA' IN MATERIA DI PROTEZIONE DEI DATI PERSONALI. ABROGAZIONE APPENDICE 5 DELLA DELIBERA DI GIUNTA REGIONALE N. 2416/2008 E SS.MM.II.

**Iter di approvazione previsto:** Delibera ordinaria

**Responsabile del procedimento:** Stefania Papili

**LA GIUNTA DELLA REGIONE EMILIA-ROMAGNA**

Premesso che:

- 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 (regolamento generale sulla protezione dei dati)" (di seguito Regolamento), a norma dell'articolo 99 "Entrata in vigore e applicazione", comma 1 dello stesso Regolamento è entrato in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta dell'Unione europea;

- l'articolo 99 comma 2 del Regolamento specifica che si applica a decorrere dal 25 maggio 2018 ed è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri;

Dato atto che il Regolamento:

- detta una complessa disciplina di carattere generale in materia di dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, comprese le pubbliche amministrazioni;

Considerato che:

- l'applicazione del nuovo Regolamento comporta modifiche ricadenti anche sull'assetto organizzativo e sulla ripartizione dei compiti e delle responsabilità in materia di protezione dei dati personali;

- per adeguarsi alle nuove disposizioni contenute nel Regolamento occorre ridefinire l'assetto complessivo dell'Ente, specificando le nuove ripartizioni delle competenze e delle responsabilità in materia di protezione dei dati personali;

Viste le delibere n. 2416/2008, Appendice 5, e n. 2169/2017, Allegato A e B, che disciplinano l'attuale assetto organizzativo dell'Ente in materia di privacy e sicurezza informatica;

Considerato che la definizione del nuovo assetto di compiti e responsabilità comporta il superamento delle disposizioni contenute negli atti di cui al periodo precedente;

Dato atto, in particolare, che la delibera 2169/2017 che designa il Responsabile della Protezione dei Dati (DPO) gli affida il mandato di dare indicazioni sulle modifiche da apportare all'Appendice 5 della delibera 2416/2008;

Visto l'Allegato A parte integrante e sostanziale della presente deliberazione formulato sulla base delle indicazioni fornite dal DPO che ridefinisce l'assetto organizzativo dell'Ente in materia di privacy e sicurezza delle informazioni, specificando, tra le altre cose, i compiti del DPO e del Responsabile del Servizio ICT relativamente alla materia;

Vista, altresì, la propria deliberazione n. 622/2017 "Approvazione della politica generale sulla sicurezza delle informazioni";

Visto il D.lgs. 14 marzo 2013, n. 33 "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" e ss.mm.ii.;

Viste le proprie deliberazioni:

- n. 2416 del 29 dicembre 2008 "Indirizzi in ordine alle relazioni organizzative e funzionali tra le strutture e sull'esercizio delle funzioni dirigenziali. Adempimenti conseguenti alla delibera 999/2008. Adeguamento e aggiornamento della delibera n. 450/2007" e ss.mm.ii, per quanto applicabile;
- n. 270 del 29 febbraio 2016 "Attuazione prima fase della riorganizzazione avviate con Delibera 2189/2015";
- n. 622 del 28 aprile 2016 "Attuazione seconda fase della riorganizzazione avviata con Delibera 2189/2015";
- n. 702 del 16 febbraio 2016 "Approvazione incarichi dirigenziali conferiti nell'ambito delle Direzioni Generali – Agenzie – Istituto, e nomina dei responsabili della prevenzione della corruzione, della trasparenza e accesso civico, della sicurezza del trattamento dei dati personali, e dell'anagrafe della stazione appaltante";
- n. 56 del 25 gennaio 2016 "Affidamento degli incarichi di Direttore Generale della Giunta regionale, ai sensi dell'art.43 della L.R. 43/2001";
- n. 1107 del 11 luglio 2016 "Integrazione delle declaratorie delle strutture organizzative della Giunta

regionale a seguito dell'implementazione della seconda fase della riorganizzazione avviata con Delibera 2189/2015";

- n. 121 del 6 febbraio 2017 "Nomina del responsabile della prevenzione della corruzione e della trasparenza";
- n. 93 del 29 gennaio 2018 di "Approvazione Piano triennale di prevenzione della corruzione. Aggiornamento 2018-2020", ed in particolare l'allegato B) "Direttiva di indirizzi interpretativi per l'applicazione degli obblighi di pubblicazione previsti dal D.lgs. n. 33 del 2013. Attuazione del piano triennale di prevenzione della corruzione 2018-2020";
- n. 468 del 10 aprile 2017 "Il sistema dei controlli interni nella regione Emilia-Romagna";

Viste le circolari del Capo di Gabinetto del Presidente della Giunta regionale PG/2017/0660476 del 13 ottobre 2017 e PG/2017/0779385 del 21 dicembre 2017 relative ad indicazioni procedurali per rendere operativo il sistema dei controlli interni predisposte in attuazione della propria deliberazione n. 468/2017;

Dato atto che il Responsabile del Procedimento ha dichiarato di non trovarsi in situazioni di conflitto, anche potenziale, di interessi;

Sentito il Servizio Sviluppo delle risorse umane e organizzazione;

Acquisiti i pareri allegati;

Su proposta dell'Assessore ai trasporti, reti infrastrutture materiali e immateriali, programmazione territoriale e agenda digitale, Raffaele Donini e dell'Assessore al Bilancio, riordino istituzionale, risorse umane e pari opportunità, Emma Petitti;

A voti unanimi e palesi;

**D E L I B E R A**

1) di approvare l'Allegato A) quale parte integrante e sostanziale della presente deliberazione;
2) di abrogare l'Appendice 5 della propria deliberazione n. 2416/2008 e ss.mm.ii., le cui disposizioni sono

integralmente sostituite da quanto approvato con il presente provvedimento;

3) di abrogare l'Allegato A e l'Allegato B della propria deliberazione n. 2169/2017;

4) di pubblicare la presente deliberazione sul Bollettino ufficiale della Regione Emilia-Romagna Telematico;

5) di dare atto, infine, che per quanto previsto in materia di pubblicità, trasparenza e diffusione di informazioni, si provvederà ai sensi delle disposizioni normative e amministrative richiamate in parte narrativa.

# ALLEGATO A
# DEFINIZIONE DI COMPETENZE E RESPONSABILITA' IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

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.

Per dare attuazione ai suddetti obblighi ed adempimenti, occorre rivedere l'assetto delle responsabilità all'interno dell'amministrazione regionale.

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

a) **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;

b) **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.

c) **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.

d) **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 e dall'articolo 29 del Regolamento, che pone l'obbligo di dare istruzioni a chi abbia accesso a dati personali e agisca sotto la titolarità del titolare o del responsabile.

Con il presente atto la Giunta:

- definisce il proprio ambito di titolarità;

- definisce le funzioni e i compiti dei Direttori generali, del Capo di Gabinetto, dei Direttori dell'Agenzia sanitaria e sociale regionale e dell'Agenzia Informazione e Comunicazione, ciascuno per il proprio ambito di competenza, per l'attuazione degli adempimenti previsti dalla normativa;

- indica i compiti assegnati al DPO designato;

- definisce i compiti della struttura competente in materia di gestione della sicurezza delle informazioni;

- definisce funzioni e compiti del Gruppo dei referenti privacy;

- definisce i criteri generali da rispettare nell'individuazione dei soggetti autorizzati a compiere le operazioni di trattamento;

delineando il complessivo ambito delle responsabilità

**2. Il titolare – Funzioni**

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è la Giunta regionale 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 alla Giunta regionale:

a) 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;

b) designare il Responsabile della protezione dei dati, specificando i compiti assegnati;

c) attribuire funzioni e compiti ai soggetti attuatori degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;

d) allocare adeguate risorse per la formazione dei dipendenti e collaboratori regionali in materia di protezione dei dati e sicurezza informatica.

**3. I Soggetti attuatori – funzioni e compiti**

Con il presente atto sono attribuiti ai soggetti attuatori funzioni e compiti per gli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dall'Ente in esecuzione del regolamento:

a) il Capo di Gabinetto, per il proprio ambito di competenza e per il trattamento di dati personali effettuato dalle strutture speciali della Giunta regionale;

b) i Direttori generali, ciascuno per il proprio ambito di competenza;

c) il Direttore dell'Agenzia Sanitaria e sociale regionale e il Direttore dell'Agenzia informazione e comunicazione, ciascuno per i trattamenti effettuati dall'Agenzia di riferimento.

d) il dirigente a cui è attribuita la competenza relativamente alle funzioni previste dal D.Lgs. n.322/1989 e alle convenzioni con l'ISTAT per l'attuazione del Programma Statistico Nazionale, per quanto riguarda i relativi trattamenti effettuati con finalità statistica.

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

Di seguito, sono indicati i compiti affidati ai soggetti 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, anche al fine di garantire un tempestivo aggiornamento del Documento Programmatico per la Sicurezza;

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; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente atto e, in particolare, facendo espresso richiamo alle policy regionali 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;

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 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) designare gli amministratori di sistema in aderenza alle norme vigenti in materia;

o) 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;

p) trasmettere al soggetto di cui al par. 3.1, le evidenze della valutazione di impatto di cui al punto precedente, ai fini della consultazione preventiva di cui all'art. 36 del Regolamento;

q) richiamare obbligatoriamente nei contratti di sviluppo di software e piattaforme, la policy regionale 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;

r) designare i Responsabili del trattamento con le modalità indicate nel paragrafo 4 del presente atto.

Nell'attuazione dei compiti sopraindicati i soggetti attuatori possono acquisire il parere del DPO nei casi e con le modalità specificate nel successivo paragrafo 7.

Fermo restando che la responsabilità delle attività sopraindicate rimane in ogni caso in capo al soggetto 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 e secondo quanto previsto, in particolare, dall'art. 39 della L.R. n. 43/2001, sono eventualmente delegabili i compiti di cui alle lettere a), b), c), d), e), f), j), l), m), n), q), r).

Tali compiti (tutti o soltanto alcuni) sono delegabili:

a) ai dirigenti responsabili di Servizio;

b) ai dirigenti assegnati alla Direzione relativamente ai trattamenti di diretta responsabilità della stessa.

### 3.1 Direttore generale competente in materia di sistemi informativi – Ulteriori compiti affidati

Al Direttore generale competente in materia di sistemi informativi spetta, inoltre:

a) l'adozione del Documento programmatico sulla sicurezza, quale compendio delle misure tecniche ed organizzative adottate dall'Ente;

b) l'adozione di disciplinari tecnici trasversali, 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;

c) la sottoscrizione e la comunicazione all'autorità di controllo degli atti di notifica e di consultazione preventiva;

d) la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

7

## 4. 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.

## 5. I soggetti autorizzati al compimento delle operazioni di trattamento (incaricati)

Sono autorizzati alle operazioni di trattamento dei dati i soggetti 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, avendo particolare attenzione ai rischi che gli stessi presentano e alla natura dei dati personali da proteggere.

Devono, altresì, essere autorizzati tutti i soggetti (di seguito "incaricati"), dipendenti e collaboratori a qualsiasi titolo, che effettuino operazioni di trattamento di dati personali sotto la diretta autorità del Titolare o dei soggetti attuatori. Gli incaricati devono essere da questi (o dai soggetti delegati come previsto al paragrafo 3) formalmente autorizzati.

Gli incaricati sono quindi designati:

a) 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;

b) 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.

L'autorizzazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento di dati personali.

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 regionali in materia di sicurezza informatica e protezione dei dati personali.

## 6. Il Responsabile della Protezione dei dati – Funzioni e compiti

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 37 e ss del suddetto regolamento, conformati alla precipua organizzazione dell'Ente:

a) 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 privacy di cui al successivo paragrafo 9;

b) 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;

c) coopera con il Garante per la protezione dei dati personali;

d) 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;

e) partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del Servizio ICT regionale o ne richiede di specifiche;

f) promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all'interno della Giunta regionale;

g) partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'Ente;

h) formula gli indirizzi per la realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento;

i) fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato al successivo paragrafo 7.

I compiti del DPO sono svolti per tutte le strutture regionali della Giunta regionale della Regione Emilia-Romagna e delle Agenzie e Istituti regionali ai sensi della lettera b), comma 3 bis, art. 1, L.R. 43/2001.

I compiti del DPO possono inoltre essere svolti per gli enti regionali ai sensi della lettera c), comma 3 bis, art. 1, L.R.

43/2001, a seguito della definizione di appositi accordi e/o convenzioni.

## 7. 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.

### 7.1 Pareri obbligatori

Devono essere obbligatoriamente richiesti pareri in ordine a:

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;

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

c) 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;

d) valutazione del rischio per i diritti e le libertà delle persone fisiche nei casi di data breach.

### 7.2 Pareri facoltativi

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

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

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

c) 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;

d) 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, con riscontro del DPO entro tre giorni.

Le richieste di parere devono essere inviate all'indirizzo di posta elettronica dpo@regione.emilia-romagna.it o nelle modalità che saranno stabilite dall'Ente.

Possono presentare le richieste di parere i soggetti attuatori o i dirigenti delegati in base ai principi generali relativi all'istituto della delega e secondo quanto previsto, in particolare, dall'art. 39 della L.R. n. 43/2001.

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 regionali 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 regionali 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 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 attuatore.

## 8. Il Servizio ICT regionale - Funzioni e compiti

Il Servizio competente in materia di sistemi informativi (di seguito anche Servizio ICT) svolge un ruolo di supporto al DPO in tema di risorse strumentali e di competenze.

In seguito alla designazione della nuova figura del DPO, le competenze assegnate al Servizio ICT regionale in materia di gestione della sicurezza delle informazioni vengono declinate come segue:

a) 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

b) cura la redazione e l’aggiornamento del Documento Programmatico per la Sicurezza sottoponendolo per l’adozione al Direttore generale competente. Le evidenze dell’analisi dei rischi sono condivise 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

c) 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;

d) 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;

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

f) garantisce il rispetto delle procedure relative alle autorizzazioni per l'accesso ai varchi controllati della Giunta regionale, a tutela del patrimonio e delle persone e a protezione dei dati personali e del patrimonio informativo dell'Ente.

Quanto sopra sostituisce i contenuti di cui all'Allegato B della delibera 2169/2017.

## 9. Il Gruppo dei referenti privacy – Funzioni e compiti

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 concerne gli adempimenti continuativi, lo studio e l'approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti anche delle nuove disposizioni normative.

Il Gruppo di referenti, già costituito con determinazione n. 2354/2008 e prorogato da ultimo con determinazione n. 2506/2017, ha i seguenti compiti:

a) supportare il soggetto attuatore della struttura di appartenenza nell'adozione delle 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;

b) costituire, nell'esecuzione del punto a), il riferimento principale per tutte le questioni che riguardano il trattamento dei dati personali della struttura di afferenza

c) supportare i soggetti attuatori, o il dirigente dallo stesso delegato, nel puntuale aggiornamento delle designazioni dei Responsabili del trattamento e degli amministratori di sistema all'interno delle strutture di appartenenza e nella costante verifica dei privilegi assegnati agli amministratori già designati;

d) supportare i Soggetti attuatori o il dirigente dallo stesso delegato, nell'aggiornamento del Registro dei trattamenti di dati personali effettuati dalle strutture di appartenenza, sulla base delle misure organizzative e delle risorse e competenze messe a disposizione dagli stessi;

e) fornire supporto alle verifiche di sicurezza svolte dal Servizio ICT e/o dal DPO nell'ambito della struttura di riferimento;

f) fornire supporto alla revisione e all'aggiornamento dei Disciplinari Tecnici regionali;

g) coordinare le richieste di parere al DPO dei soggetti attuatori di propria afferenza nei casi e con le modalità previsti dal presente atto.

Fanno parte del Gruppo privacy anche i referenti dell'Assemblea Legislativa e delle Agenzie e Istituti regionali con autonoma titolarità.

Il coordinamento del Gruppo è demandato al Servizio ICT regionale, che cura l'aggiornamento dei componenti, sulla base delle comunicazioni provenienti dalle diverse strutture.

## 10. Disciplina dei rapporti tra DPO, strutture regionali della Giunta e R.P.C.T in materia accesso civico generalizzato

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il DPO, le strutture regionali della Giunta, 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 regionali 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.

In aderenza al punto c) del paragrafo 7.2, il DPO, inoltre, su richiesta delle strutture regionali, 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.

In aderenza al punto d) del paragrafo 7.2, il DPO, su richiesta delle strutture regionali, 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 regionali 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.

REGIONE EMILIA-ROMAGNA
Atti amministrativi

GIUNTA REGIONALE

Stefania Papili, Responsabile del SERVIZIO ICT REGIONALE esprime, ai sensi dell'art. 37, quarto comma, della L.R. n. 43/2001 e della deliberazione della Giunta Regionale n. 2416/2008 e s.m.i., parere di regolarità amministrativa di legittimità in relazione all'atto con numero di proposta GPG/2018/1131

IN FEDE

Stefania Papili

REGIONE EMILIA-ROMAGNA
Atti amministrativi

GIUNTA REGIONALE

Francesco Raphael Frieri, Direttore generale della DIREZIONE GENERALE RISORSE, EUROPA, INNOVAZIONE E ISTITUZIONI esprime, ai sensi dell'art. 37, quarto comma, della L.R. n. 43/2001 e della deliberazione della Giunta Regionale n. 2416/2008 e s.m.i., parere di regolarità amministrativa di merito in relazione all'atto con numero di proposta GPG/2018/1131

IN FEDE

Francesco Raphael Frieri

OMISSIS

---

L'assessore Segretario

Bianchi Patrizio

---

Servizi Affari della Presidenza

Firmato digitalmente dal Responsabile Roberta Bianchedi