

# REGIONE EMILIA-ROMAGNA

## Atti amministrativi GIUNTA REGIONALE

Delibera Num. 2169 del 20/12/2017

Seduta Num. 47

**Questo** mercoledì 20 **del mese di** dicembre

**dell' anno** 2017 **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) Gazzolo Paola	Assessore
7) Mezzetti Massimo	Assessore
8) Petitti Emma	Assessore
9) Venturi Sergio	Assessore

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

**Proposta:** GPG/2017/2293 del 18/12/2017

**Struttura proponente:** SERV. SVILUPPO DELLE RISORSE UMANE DELLA GIUNTA REGIONALE E DEL SISTEMA DEGLI ENTI DEL SSR  
DIREZIONE GENERALE RISORSE, EUROPA, INNOVAZIONE E ISTITUZIONI

**Assessorato proponente:** ASSESSORE AL BILANCIO, RIORDINO ISTITUZIONALE, RISORSE UMANE E PARI OPPORTUNITÀ

**Oggetto:** PRIMI ADEGUAMENTI AL REGOLAMENTO (UE) 2016/679: DEFINIZIONE ORGANIZZATIVA E DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

**Iter di approvazione previsto:** Delibera ordinaria

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) prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO)
- l'art. 39 dello stesso Regolamento prevede in capo a tale figura i seguenti compiti:
  - a) *"informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;*
  - b) *sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento 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) *fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35*
  - d) *cooperare con l'autorità di controllo*
  - e) *fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione*

Precisato che il Regolamento, entrato in vigore il 24/5/2016, si applicherà dal 28/5/2018 e che per questa data l'Ente deve adeguarsi alle nuove disposizioni effettuando scelte organizzative e tecnologiche sulla scorta delle

indicazioni del DPO, atteso che il mancato adempimento è sanzionabile ai sensi dell'art. 83 comma 4 del Regolamento;

Considerato quindi che sussiste la necessità di provvedere al più presto alla individuazione del soggetto cui affidare i suddetti compiti e responsabilità;

Visti gli artt. 37 commi 3, 5, 6 e 7 e 38 commi 1, 2, 3, 5 e 6 che definiscono le modalità di designazione del Responsabile della protezione dei dati e alcune indicazioni sulla sua posizione come segue:

- nel caso di autorità pubbliche o organismi pubblici, il responsabile della protezione dati può essere designato per più di esse, tenuto conto della loro struttura organizzativa e dimensione;

- il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39;

- il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi;

- i dati di contatto del responsabile della protezione dei dati devono essere pubblicati e comunicati all'autorità di controllo da parte del titolare del trattamento o del responsabile del trattamento;

- il responsabile della protezione dei dati deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;

- al responsabile della protezione dei dati debbono essere fornite le risorse necessarie per assolvere i propri compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;

- il responsabile della protezione dei dati non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti suddescritti;

- il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti;

- il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento;
- il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri;
- il responsabile della protezione dei dati può svolgere altri compiti e funzioni; il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi;

Viste, inoltre, le linee-guida sui responsabili della protezione dei dati definite dal gruppo di lavoro articolo 29 in materia di protezione dei dati personali istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 nella versione emendata e adottata in data 5 aprile 2017;

Dato atto che:

- I criteri per l'individuazione del responsabile della protezione dei dati previsti dal richiamato co. 5, art. 37, Regolamento sono, sinteticamente, le qualità professionali, la conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e la capacità di assolvere i compiti previsti dal Regolamento stesso;
- Relativamente ai suddetti criteri, le sopracitate linee guida definite dal gruppo di lavoro articolo 29 in materia di protezione dei dati personali istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, non offrono dettagliate definizioni, ma sottolineano, oltre all'importanza della padronanza della normativa di settore europea e nazionale, la rilevanza della conoscenza del contesto organizzativo, delle operazioni di trattamento e delle problematiche in materia di protezione dei dati del titolare del trattamento, delle norme e procedure amministrative applicabili e il rilievo di qualità professionali, quali l'integrità e elevati standard deontologici;
- Alla luce di tali linee guida, si ritiene privilegiare la designazione del responsabile della protezione dei dati nell'ambito dei dirigenti, preferibilmente di ruolo, con incarichi di responsabilità di posizione e struttura nelle strutture ordinarie della Giunta regionale;

- Il dirigente incaricato come responsabile della protezione dei dati non deve essere in situazione di conflitto d'interessi, che, alla luce delle richiamate linee guida, si configura nel caso in cui lo stesso sia anche responsabile di definire le finalità e/o le modalità del trattamento dei dati personali e/o di rappresentare il titolare o il responsabile del trattamento in giudizio;
- È stata esaminata la banca dati dell'Osservatorio delle competenze della Dirigenza;

Valutato che il dott. Ing. Alessandro Zucchini, attualmente Responsabile del Servizio *Coordinamento politiche di accesso ai servizi digitali per imprese e cittadini*:

- sia in possesso dei requisiti di cui sopra, in quanto è un dirigente di ruolo, con un'adeguata preparazione culturale di base; con esperienze pluriennali in vari ruoli dell'Amministrazione che gli hanno permesso di acquisire un'approfondita conoscenza sulla complessità e sull'articolazione organizzativa della Regione, sul suo specifico contesto amministrativo di riferimento, sulle sue tipologie e operazioni di trattamento;

- sia in possesso delle capacità per poter svolgere i compiti previsti dal Regolamento alla luce dell'ampio e articolato ventaglio di esperienze professionali maturate;

Accertato che non sussistono conflitti di interessi, come richiesti dal Regolamento UE, in quanto il dott. Ing. Alessandro Zucchini, in ragione dell'incarico Responsabile del Servizio *Coordinamento politiche di accesso ai servizi digitali per imprese e cittadini* non ha il potere di definire le finalità e/o le modalità del trattamento dei dati personali e/o di rappresentare il titolare o il responsabile del trattamento in giudizio;

Acquisita agli atti del procedimento con protocollo PG/772561 del 18/12/2017 la dichiarazione sostitutiva di certificazione sull'assenza di conflitti di interessi rispetto all'assunzione dell'incarico aggiuntivo di Responsabile della protezione dei dati, per quanto riguarda le disposizioni dettate dalla normativa nazionale e regionale in materia (in particolare fissati dal Codice di comportamento dei pubblici dipendenti);

Ritenuto, pertanto necessario, procedere alla designazione del dott. Ing. Alessandro Zucchini, quale Responsabile della protezione dei dati e alla definizione delle caratteristiche organizzative di tale ruolo in

relazione all'assetto delle funzioni e responsabilità dell'Amministrazione regionale;

Vista la deliberazione n. 2416/2008 che istituisce, per la Giunta regionale, la figura del Responsabile della Sicurezza e, specificatamente, nella sezione 5 dell'Appendice 5 ne definisce i compiti che, in parte, si sovrappongono a quelli che oggi la normativa comunitaria assegna al DPO;

Preso atto che l'incarico di Responsabile della Sicurezza è stato assegnato con deliberazione n. 702/2016 alla dirigente del Servizio ICT Regionale, che lo svolge anche con il supporto di risorse assegnate alla struttura;

Ritenuto necessario, per quanto in precedenza esposto, rivedere l'attuale assetto organizzativo per renderlo conforme a quanto previsto dalla normativa comunitaria apportando le necessarie modifiche alla declaratoria del Servizio ICTR e alle declaratorie delle Posizioni Organizzative interessate;

Visto inoltre:

l'art. 45 del D. L. 9 febbraio 2012, n. 5 "Disposizioni urgenti in materia di semplificazione e di sviluppo", che abroga la lettera g) del comma 1 e i paragrafi da 19 a 19.8 e il paragrafo 26 dell'allegato B del Codice che prevedeva, come "misura minima" obbligatoria, la redazione di un Documento Programmatico sulla Sicurezza;

Considerato che la nuova normativa europea impone l'adozione di misure di sicurezza adeguate ed efficaci (art. 24 Regolamento 2016/679) e il Documento Programmatico della Sicurezza costituisce il compendio delle misure adottate nell'Ente;

Ritenuto pertanto di continuare, per la suddetta finalità, a redigere, con cadenza annuale, il DPS ancorché non più obbligatorio;

Premesso inoltre che:

- l'art. 50 del d.lgs. 82/2005 (Codice dell'amministrazione digitale) stabilisce che
  - o *"I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati";*

- o *"Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo per la prestazione di elaborazioni aggiuntive";*
- ai sensi dell'articolo 43 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le pubbliche amministrazioni che procedono all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive presentate dai cittadini, accedono esclusivamente in via telematica alle banche dati delle amministrazioni certificanti;
- al fine di agevolare l'acquisizione d'ufficio le suddette informazioni, le amministrazioni certificanti sono tenute a consentire alle amministrazioni procedenti, senza oneri, la consultazione per via telematica dei loro archivi informatici, nel rispetto della riservatezza dei dati personali;
- ai sensi dell'art. 72 comma 1 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le Pubbliche Amministrazioni sono tenute a designare un soggetto Responsabile per le attività volte a gestire, garantire e verificare la trasmissione dei dati o l'accesso diretto agli stessi da parte delle amministrazioni procedenti;
- ai sensi dell'art. 72 comma 2 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, Le amministrazioni certificanti, per il tramite dell'ufficio di cui al comma 1, individuano e rendono note, attraverso la pubblicazione sul sito istituzionale dell'amministrazione, le misure organizzative adottate per l'efficiente, efficace e tempestiva acquisizione d'ufficio dei dati e per l'effettuazione dei controlli medesimi, nonché le modalità per la loro esecuzione;
- il Piano triennale per la prevenzione della corruzione e la trasparenza 2017-2019, approvato con deliberazione n. 89 del 2017, individua tale responsabilità in capo al "Servizio ICT regionale";

Considerato che in capo al Servizio ICT regionale è riconosciuta la competenza e la responsabilità in ordine agli

aspetti tecnologici della trasmissione dei dati o dell'accesso diretto agli stessi da parte delle altre amministrazioni;

Considerato, altresì, che la responsabilità della messa a disposizione dei dati, della corretta fruibilità degli stessi e della sottoscrizione degli accordi atti a disciplinare tale trasmissione deve, invece, riconoscersi in capo alle Direzioni Generali della Giunta della Regione Emilia-Romagna cui afferiscono le strutture che gestiscono le singole banche dati;

Acquisito il parere allegato;

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 segreti;

#### D E L I B E R A

- 1) di designare, dal 01/01/2018, quale Responsabile della protezione dei dati (DPO) per la Giunta regionale il dirigente regionale Alessandro Zucchini, che risulta in possesso delle necessarie qualificazioni ed esperienze come esposto in premessa;
- 2) di specificare le caratteristiche organizzative e i compiti assegnati al DPO come indicato nell'allegato A, parte integrante e sostanziale del presente atto;
- 3) di specificare come indicato nell'Allegato B i compiti che, nelle more della più puntuale ridefinizione di funzioni e responsabilità di cui al successivo punto 8), afferiscono al Responsabile del Servizio ICT Regionale, dal 01/01/2018;
- 4) di stabilire che il Direttore generale competente approvi, con cadenza annuale, il Documento programmatico sulla Sicurezza, quale compendio delle misure tecniche ed organizzative adeguate ai sensi del Regolamento Europeo 2016/679;
- 5) di modificare, dal 01/01/2018, la declaratoria del Servizio ICT regionale come indicato in allegato C;
- 6) di dare atto che il Direttore competente provvederà, con propri atti, agli eventuali adeguamenti organizzativi in

relazione al nuovo assetto delle funzioni e competenze definite con il presente provvedimento;

- 7) di stabilire la cessazione della validità, dal 01/01/2018, della sezione 5 dell'Appendice 5 della delibera 2416/2008;
- 8) di dare atto che l'incarico di Responsabile della Sicurezza attribuito alla dott.ssa Stefania Papili con deliberazione n. 702/2016, cessa per effetto di quanto disposto al precedente punto 7) dalla data del 01/01/2018;
- 9) di dare mandato al DPO nominato con il presente provvedimento di dare indicazioni sulle modifiche da apportare all'Appendice 5 della Delibera 2416/2008, per l'adeguamento dell'assetto organizzativo dell'Ente, in materia di privacy e sicurezza delle informazioni alla nuova disciplina;
- 10) di individuare il Servizio ICT Regionale quale ufficio responsabile per gli aspetti tecnologici della trasmissione dei dati o dell'accesso diretto agli stessi da parte delle altre amministrazioni ai sensi dell'art. 72 co.1 DPR 445/2000;
- 11) di individuare nelle Direzioni Generali della giunta della regione Emilia Romagna cui afferiscono le strutture che gestiscono le singole banche dati la responsabilità della messa a disposizione dei dati, della corretta fruibilità degli stessi e della sottoscrizione degli accordi atti a disciplinare tale trasmissione;
- 12) di dare atto che Direttore generale *Risorse, Europa, innovazione e Istituzioni* assicurerà la pubblicazione dei dati di contatto del DPO sul sito internet della Regione e su Amministrazione Trasparente e la comunicazione al Garante per la protezione dei dati personali.

CRITERI PER LA DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Fermo restando quanto stabilito dalla normativa europea e nazionale in materia, si prevedono i seguenti ulteriori criteri nell'individuazione del DPO:

- la scelta è compiuta, in prima istanza, nell'ambito dei dirigenti, con incarichi di responsabilità di struttura o posizione dirigenziale presso le strutture ordinarie della Giunta regionale;
- elemento preferenziale è essere dirigente di ruolo dell'Amministrazione regionale;
- la designazione del DPO tramite contratto di servizio è una soluzione residuale.

MODALITA' DI INDIVIDUAZIONE DEL DPO

Il titolare del trattamento è responsabile della designazione del DPO. Nell'attuale assetto delle responsabilità, tale competenza è della Giunta regionale che provvede tramite proprio atto.

Nel caso di designazione esterna del DPO, il relativo accordo di servizio definirà le modalità organizzative e operative per lo svolgimento delle funzioni proprie del DPO.

DESIGNAZIONE INTERNA DEL DPO: CARATTERISTICHE ORGANIZZATIVE E AMBITO DI COMPETENZA

Il ruolo di DPO si configura come un incarico aggiuntivo a quello principale.

Tale incarico aggiuntivo non comporta alcuna modifica all'incarico principale, al relativo contratto di lavoro, anche in termini economici. La sua durata non eccede quella dell'incarico principale.

Il DPO, nello svolgimento delle sue funzioni, si rapporta direttamente con l'organo d'indirizzo politico, anche per l'espressione dei pareri di regolarità amministrativa in ordine alle eventuali proposte di atti che, il dirigente con

tale incarico aggiuntivo, dovrà presentare alla Giunta regionale.

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.

Inoltre i compiti del DPO possono 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.

#### COMPITI DEL DPO

- a) informa e fornisce consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, coordinando il gruppo dei referenti designati dalle strutture
- b) sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell'Ente, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) fornisce il proprio parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento ai sensi dell'articolo 35 del Regolamento 2016/679;
- d) coopera con il Garante per la protezione dei dati personali;
- e) 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;
- f) fornisce supporto all'Ente nella definizione delle linee guida in materia di protezione dei dati personali e sicurezza delle informazioni, esprimendo formale parere;
- g) partecipa alla progettazione di nuove applicazioni o alla modifica sostanziale di quelle esistenti in aderenza al principio della privacy by design;

- h) fornisce supporto alla redazione e aggiornamento dei disciplinari tecnici trasversali e di settore, esprimendo formale parere;
- i) fornisce supporto e coopera con la struttura competente nei casi di incidenti di sicurezza;
- j) vigila sulla puntuale osservanza della normativa e delle policy regionali in materia di sicurezza delle informazioni e di trattamento di dati personali, partecipando allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del Servizio ICT regionale o richiedendone di specifiche;
- k) 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;
- l) fornisce supporto nella definizione delle misure più idonee ed efficaci a garantire l'esercizio dei diritti degli interessati di cui al Capo III del Regolamento;
- m) formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento

**COMPITI DEL RESPONSABILE DEL SERVIZIO ICT REGIONALE**

In quanto responsabile del sistema di gestione della sicurezza delle informazioni:

- a) individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente, acquisendo il preventivo parere del DPO in particolare sulle seguenti attività:
  - ~ redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali
  - ~ 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
- 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;
  - ~ notificare l'eventuale violazione dei dati personali 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;

<b>Codice</b>	00000435
<b>Denominazione</b>	SERVIZIO ICT REGIONALE
<b>Struttura padre</b>	DIREZIONE GENERALE RISORSE, EUROPA, INNOVAZIONE E ISTITUZIONI (codice D0000032)
<b>Famiglia professionale</b>	Attivatore di azioni innovative
<b>Area settoriale omogenea</b>	Tecnologie dell'informazione e della comunicazione (ICT)
<b>Declaratoria</b>	<p>Promuove lo sviluppo di servizi ICT adeguati alla realizzazione di un'amministrazione digitale aperta, integrata, efficiente ed efficace</p> <p>Garantisce il supporto al cambiamento organizzativo dell'Ente tramite l'individuazione, lo sviluppo, il dispiegamento e la gestione di tecnologie ICT, anche tramite soluzioni in cloud, funzionali a promuovere processi digitali e dematerializzati e nuovi modelli di lavoro</p> <p>Predisporre il piano triennale e annuale di informatizzazione dell'ente per assicurare la coerenza di tutte le iniziative ICT dell'ente con i processi di sviluppo istituzionale e organizzativo</p> <p>Garantisce il monitoraggio dei servizi ICT dell'ente al fine di individuare azioni migliorative dei livelli di automazione e digitalizzazione</p> <p>Progetta, dispiega e gestisce le infrastrutture informatiche e telematiche dell'ente e ne cura la manutenzione e l'evoluzione tecnologica negli ambiti: sistemi centrali e dipartimentali, data base, attrezzature per l'automazione d'ufficio fisse e mobili, rete locali e geografiche, sistemi web, posta elettronica, piattaforme di condivisione e collaborazione</p> <p>Gestisce la Telefonia fissa e mobile dell'ente Regione e ne studia le possibilità di sviluppo tecnologico ed integrazione con le infrastrutture di rete locale e geografica</p> <p>Individua e definisce standard e piattaforme tecnologiche a supporto delle filiere applicative su cui si sviluppa il sistema informativo dell'ente Regione</p> <p>Progetta e realizza i sistemi informativi di supporto alle funzioni amministrative dell'Ente; progetta e realizza, in concorso con le Direzioni generali richiedenti, sistemi informativi settoriali e multisetoriale per le strutture regionali</p> <p>Cura il ciclo di vita dei sistemi realizzati, assicurandone la manutenzione evolutiva, l'adeguamento tecnologico, la manutenzione della documentazione e verificando la qualità dei prodotti realizzati, anche nell'ottica di garantire la sicurezza delle applicazioni informatiche</p> <p>Certifica la coerenza delle procedure sviluppate esternamente al Servizio con gli standard regionali, anche nell'ottica di garantire la sicurezza delle applicazioni informatiche, attraverso verifiche di qualità preventive e finali sui progetti e sui prodotti realizzati e attraverso procedure e protocolli omogenei per il passaggio in produzione delle applicazioni</p> <p>Fornisce assistenza agli utenti del sistema informativo dell'ente Regione; in particolare gestisce il supporto per i sistemi informativi a supporto alle funzioni trasversali dell'Ente e dei sistemi informativi strategici a valenza multisetoriale</p> <p>Definisce e verifica l'usabilità e l'accessibilità dei sistemi informativi dell'ente Regione, promuovendo anche attività di informazione e sensibilizzazione</p> <p>Garantisce il governo, la gestione e il presidio dei sistemi di autenticazione ed autorizzazione all'accesso fisico e logico alle risorse informatiche e amministra</p>

	<p>strumenti e procedure atte a garantire la sicurezza del Sistema informativo regionale</p> <p>Coadiuvata, per quanto di competenza, il Responsabile della Protezione dei dati (Data Protection Officer) dell'ente nell'esercizio delle funzioni attribuite dalla legge</p> <p>E' responsabile del sistema di gestione della sicurezza delle informazioni e individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente</p> <p>Cura la progettazione, lo sviluppo, la gestione e l'evoluzione dei sistemi informativi geografici e della relativa infrastruttura tecnologica di supporto</p> <p>Definisce le regole per le applicazioni integrate con l'infrastruttura geografica regionale, fornendo supporto agli sviluppatori; cura i servizi informatici funzionali alle esigenze di condivisione, fruizione, accesso, elaborazione, produzione e pubblicazione dell'informazione geografica da parte delle altre Direzioni e agenzie regionali</p> <p>Presidia l'attuazione del modello organizzativo per la governance dei sistemi informativi regionali coordinando le strutture regionali nella definizione della programmazione unitaria di risorse ICT, identificando soluzioni tecniche e servizi comuni, definendo standard tecnologici e livelli di servizio</p> <p>Partecipa al processo di attuazione dell'Agenda digitale regionale per gli aspetti relativi ai sistemi informativi compresi nella programmazione unitaria ICT</p> <p>Cura i rapporti con Lepida S.p.A. quale riferimento per l'acquisizione da parte della Regione di servizi offerti dalla società</p> <p>E' responsabile, per gli aspetti tecnologici, della trasmissione dei dati e dell'accesso diretto agli stessi da parte delle altre Amministrazioni</p>
--	--

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 in merito all'atto con numero di proposta GPG/2017/2293

IN FEDE

Francesco Raphael Frieri

**REGIONE EMILIA-ROMAGNA**

**Atti amministrativi**

**GIUNTA REGIONALE**

Delibera Num. 2169 del 20/12/2017

Seduta Num. 47

OMISSIS

---

L'assessore Segretario

Bianchi Patrizio

---

Servizi Affari della Presidenza

Firmato digitalmente dal Responsabile Roberta Bianchedi