CONSIGLIO REGIONALE DEL LAZIO

UFFICIO DI PRESIDENZA

Deliberazione n. 60 del 12 giugno 2018

OGGETTO: *Regolamento (UE) 2016/679: definizione organigramma privacy del Consiglio regionale in conformità con lo stesso. Approvazione modifiche al regolamento di organizzazione del Consiglio regionale e Linee guida per il trattamento dei dati personali.*

Schema di deliberazione n. 45 del 12 giugno 2018

Verbale n. 14

Componenti:

			Pres.	Ass.	
Presidente	Daniele	LEODORI	x	☐	_____
Vice Presidente	Adriano	PALOZZI	x	☐	_____
Vice Presidente	Devid	PORRELLO	x	☐	_____
Consigliere Segretario	Michela	DI BIASE	x	☐	_____
Consigliere Segretario	Daniele	GIANNINI	x	☐	_____
Consigliere Segretario	Gianluca	QUADRANA	x	☐	_____

VISTO PER IL PARERE DI REGOLARITA' TECNICO-AMMINISTRATIVA

IL DIRIGENTE/IL DIRETTORE

_____

VISTO PER IL PARERE DI REGOLARITA' CONTABILE

IL DIRIGENTE/IL DIRETTORE

_____

☐ **RILEVA** ☐ **NON RILEVA**

Assiste il Segretario generale dott.ssa Cinzia Felci

L'UFFICIO DI PRESIDENZA

Su proposta del Presidente

VISTO lo Statuto, approvato con legge statutaria 11 novembre 2004, n. 1 e successive modifiche;

VISTA la legge regionale 18 febbraio 2002, n. 6 (Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza ed al personale regionale) e successive modifiche;

VISTO il regolamento di organizzazione del Consiglio regionale, approvato con deliberazione dell'Ufficio di presidenza 29 gennaio 2003, n. 3 e successive modifiche;

VISTA la determinazione del Segretario generale 28 gennaio 2014, n. 45 (Istituzione delle aree, degli uffici e delle funzioni direzionali di staff presso il Consiglio regionale. Revoca delle determinazioni 13 ottobre 2010, n. 806 e successive modifiche e 16 maggio 2011, n. 312 e successive modifiche) e successive modifiche;

VISTA la propria deliberazione 22 maggio 2018, n. 46, con la quale la Dott.ssa Cinzia Felci è stata nominata Segretario generale del Consiglio regionale;

VISTO il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di dati personali) e successive modifiche;

VISTO 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 denominato RGPD, che, nell'ambito del CAPO IV (Titolare del trattamento e responsabile del trattamento), Sezioni 1 (Obblighi generali), 2 (Sicurezza dei dati personali) e 4 (Responsabile della protezione dei dati), disciplina, tra l'altro, l'obbligo di tenuta di un registro delle attività di trattamento dei dati personali, di un registro delle violazioni degli stessi e la figura del Responsabile della protezione dei dati, per il seguito RPD;

VISTI del RGPD, in particolare:

— l'articolo 4, ai sensi del quale:

- per "*titolare del trattamento*" si intende 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; ...*" (paragrafo 1., n. 7));
- "*responsabile del trattamento*" è "*…la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*" (paragrafo 1., n. 8));
- con il termine "*trattamento*" ci si riferisce a "*.... qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;*" (paragrafo 1., n. 2));

— l'articolo 13, che disciplina le informazioni che, per garantire un trattamento corretto e trasparente, il titolare del trattamento è tenuto a fornire all'interessato rispetto ai dati personali di quest'ultimo che detiene;

— l'articolo 30, a termini del quale:
- "*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:*
  a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
  b) le finalità del trattamento;
  c) una descrizione delle categorie di interessati e delle categorie di dati personali;
  d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
  e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1." (paragrafo 1.);

- "*Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:*
  a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
  b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
  c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
  d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1." (paragrafo 2.);
- "*I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.*" (paragrafo 3.);

— l'articolo 37, a norma del quale "*Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:*
  a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; ..." (paragrafo 1., lettera a));

— l'articolo 38, ai sensi del quale "*Il titolare del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.*" (paragrafo 2.);

— l'articolo 39, secondo cui il RPD "*... è incaricato almeno dei 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." (paragrafo 1.);

— l'articolo 99, in base al quale:

- il RGPD "*..... entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.*" (paragrafo 1.);
- "*Esso si applica a decorrere dal 25 maggio 2018…"* ed *"… è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.*" (paragrafo 2.);

VISTA la legge 25 ottobre 2017, n. 163 (Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017) e, in particolare, l'articolo 13, ai sensi del quale il Governo è delegato all'adozione di uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del RGPD;

ATTESO che al momento non è stata adottata dal Governo la normativa di cui sopra;

CONSIDERATO che il RGPD ha introdotto diverse novelle in materia di protezione dei dati personali con la conseguenza che, sia pure in pendenza dell'adozione della ricordata normativa statale, si rendono necessari, per meglio adeguarvisi, una serie di aggiornamenti di tipo

organizzativo del Consiglio regionale, finanche concernenti il quadro delle competenze interne;

CONSIDERATO in particolare, il principio di "responsabilizzazione" ("*accountability*") che attribuisce, al titolare del trattamento, il compito di mettere in atto *"misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento"*, alla luce "*della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche"* (articolo 24, paragrafo 1. del RGPD);

RITENUTO pertanto di introdurre gli aggiornamenti di cui sopra attraverso, in particolare:

— apposite modifiche al regolamento di organizzazione del Consiglio regionale, contenute nell'allegato A alla presente deliberazione e limitate in questa fase - tenuto conto della ricordata mancata adozione, ad oggi, della normativa di adeguamento del quadro normativo nazionale alle nuove disposizioni europee - alla abrogazione e sostituzione degli articoli del Capo VI (Il trattamento dei dati personali) del Titolo IX (Tutele e garanzie) ovvero all'inserimento in esso di nuovi articoli, al fine di dare applicazione al RGPD, anche attraverso la soppressione delle disposizioni che con lo stesso si pongono in contrasto. Tali modifiche, prevedono, tra l'altro, l'istituzione del "*Gruppo di Lavoro Privacy*", con compiti operativi di analisi, gestione e soluzione dei problemi applicativi del RGPD nonché per l'individuazione di soluzioni tecniche tese a prevenire e contrastare i rischi connessi alla sicurezza informatica correlati alla protezione dei dati personali;
— l'approvazione di un documento denominato *"Linee guida per il trattamento dei dati personali*", contenuto nell'allegato B alla presente deliberazione;

RITENUTO altresì di demandare al Segretario generale l'approvazione dell'informativa, ex articolo 13 del RGPD, che il titolare del trattamento è tenuto a fornire agli utenti, identificati o identificabili, del portale web ufficiale del Consiglio regionale - ossia coloro che lo consultano e interagiscono con esso e con i servizi web regionali accessibili per via telematica - in riferimento al trattamento dei dati personali degli stessi utenti;

VISTO l'articolo 1, comma 116, lettera c) della legge regionale 13 agosto 2011, n. 12, che richiede la pubblicazione sul Bollettino ufficiale della Regione, tra gli altri, dei provvedimenti degli organi regionali di

direzione politica laddove prevista da leggi, regolamenti ovvero dal dispositivo dei provvedimenti stessi;

VISTO il decreto legislativo 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 successive modifiche e, in particolare, l'articolo 12, comma 1;

all'unanimità dei presenti

DELIBERA

per i motivi espressi in premessa, che costituiscono parte integrante e sostanziale della presente deliberazione

1. di approvare apposite modifiche al regolamento di organizzazione del Consiglio regionale, contenute nell'allegato A alla presente deliberazione, di cui costituisce parte integrante e sostanziale, limitate in questa fase alla abrogazione e sostituzione degli articoli del Capo VI (Il trattamento dei dati personali) del Titolo IX (Tutele e garanzie) ovvero all'inserimento in esso di nuovi articoli, al fine di dare applicazione al RGPD anche attraverso la soppressione delle disposizioni che con lo stesso si pongono in contrasto;

2. di approvare il documento denominato *"Linee guida per il trattamento dei dati personali*", contenuto nell'allegato B alla presente deliberazione, di cui costituisce parte integrante e sostanziale;

3. di demandare al Segretario generale l'approvazione dell'informativa, ex articolo 13 del RGPD, che il titolare del trattamento è tenuto a fornire agli utenti, identificati o identificabili, del portale web ufficiale del Consiglio regionale in riferimento al trattamento dei dati personali degli stessi;

4. di pubblicare la presente deliberazione nel Bollettino ufficiale della Regione e nella pertinente sottosezione della sezione "Amministrazione Trasparente" del sito web del Consiglio regionale nonché nell'ulteriore sezione dello stesso all'uopo dedicata;

5. di demandare alle strutture competenti ogni successivo e consequenziale adempimento, ivi compresa la trasmissione della presente deliberazione ai direttori dei servizi, agli altri dirigenti e al RPD.

IL SEGRETARIO
F.to Cinzia Felci

IL PRESIDENTE
F.to Daniele Leodori

Allegato A alla deliberazione dell'Ufficio di presidenza 12 giugno 2018, n. 60

Modifiche al Capo VI del Titolo IX del regolamento di organizzazione del Consiglio regionale, approvato con deliberazione dell'Ufficio di presidenza 29 gennaio 2003, n. 3 e successive modifiche

Al regolamento di organizzazione del Consiglio regionale, approvato con deliberazione dell'Ufficio di presidenza 29 gennaio 2003, n. 3 e successive modifiche, sono apportate le seguenti modifiche:

1. L'articolo 407 è sostituito dal seguente:

"**Art. 407**
(Oggetto)

1. Le disposizioni di cui al presente capo disciplinano il trattamento dei dati personali contenuti nelle banche dati organizzate, gestite o utilizzate dal Consiglio regionale, in conformità con 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 denominato RGPD, e con il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di dati personali) e successive modifiche, di seguito denominato Codice.".

2. L'articolo 408 è sostituito dal seguente:

"**Art. 408**
(Finalità)

1. Il Consiglio regionale garantisce che il trattamento dei dati personali si svolga per il raggiungimento delle sue finalità istituzionali, nel rispetto dei principi definiti dal Capo II del RGPD e dal Codice. In tale ottica, il Consiglio regionale agevola la trasmissione di dati e documenti tra le banche dati e gli archivi dello stesso nonché tra questi e quelli degli enti territoriali, degli enti pubblici, dei gestori, degli esercenti e degli incaricati di pubblico servizio, anche al fine di adempiere all'obbligo di comunicazione interna ed esterna e di semplificazione dell'azione amministrativa.

2. La trasmissione dei dati può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità.

3. Ai fini del presente Capo, per finalità istituzionali si intendono sia le funzioni attribuite al Consiglio regionale dallo Statuto, dalle leggi e dai regolamenti, sia quelle esercitate dallo stesso a seguito di deleghe, intese, accordi, convenzioni o concessioni. In detti casi, la trasmissione di dati o documenti tra i soggetti interessati, anche privati, è preceduta da uno specifico protocollo d'intesa che contenga, di

norma, l'indicazione del titolare e del responsabile del trattamento nonché le modalità di connessione, trasferimento e comunicazione dei dati.".

3. L'articolo 409 è abrogato;

4. L'articolo 410 è abrogato;

5. L'articolo 411 è sostituito dal seguente:

"**Art. 411**
(Titolare del trattamento dei dati personali. Compiti)

1. Il titolare del trattamento dei dati personali, di seguito denominato Titolare, è, ai sensi dell'articolo 4, paragrafo 1., numero 7) del RGPD, il Consiglio regionale, cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.".

6. Dopo l'articolo 411 sono inseriti i seguenti:

"**Art. 411 bis**
(Delegati e persone autorizzate al trattamento dei dati personali. Compiti)

1. I delegati al trattamento dei dati personali, di seguito denominati Delegati, conformemente con gli articoli 28 e 29 del RGPD, sono i dirigenti e i titolari di incarichi di funzione dirigenziale, comunque denominati, che comportano l'esercizio delle competenze di amministrazione e gestione, ciascuno per la parte di propria competenza.

2. Relativamente alle strutture di diretta collaborazione degli organi istituzionali, degli organi di controllo e garanzia e degli organi politici di cui all'articolo 3 del presente regolamento, i Delegati sono così individuati:

a) per le strutture di diretta collaborazione del Presidente del Consiglio, nella figura del Capo dell'Ufficio di Gabinetto di cui all'articolo 5;

b) per le strutture di diretta collaborazione dei restanti componenti dell'Ufficio di presidenza, nel rispettivo responsabile di cui all'articolo 8, comma 2;

c) per le strutture dei Presidenti delle commissioni consiliari permanenti e speciali e del Comitato regionale di controllo contabile, nel rispettivo responsabile di cui all'articolo 9, comma 2;

d) per la struttura del Presidente del Comitato per il monitoraggio dell'attuazione delle leggi e la valutazione degli effetti delle politiche regionali, nel rispettivo responsabile di cui alla legge regionale 8 giugno 2016, n. 7 (Istituzione del Comitato per il monitoraggio dell'attuazione delle leggi e la valutazione degli effetti delle politiche regionali);

e) per la struttura di diretta collaborazione dei gruppi consiliari, è individuato nel presidente dello stesso o da soggetto da questi individuato all'interno della medesima struttura;

f) per la struttura di diretta collaborazione dei componenti della Conferenza dei presidenti, da ciascun componente della stessa per quanto di rispettiva competenza o da soggetto da questi individuato all'interno della medesima struttura;

g) per la struttura di diretta collaborazione degli organismi regionali prevista da specifiche disposizioni di legge, è individuato nel presidente o da altro organo monocratico degli stessi organismi o da soggetto da questi individuato all'interno della medesima struttura;

3. Le persone autorizzate al trattamento dei dati personali, di seguito denominati Persone autorizzate, conformemente con gli articoli 4, paragrafo 1., numero 10) e 28, paragrafo 3., lettera b) del RGPD, sono i dipendenti formalmente autorizzati al trattamento di dati personali dai Delegati, con specifica individuazione dell'ambito del trattamento consentito, sul presupposto dell'assegnazione alla relativa struttura organizzativa.

4. I Delegati e le Persone autorizzate provvedono al trattamento di dati personali nei termini e con le modalità di cui alle relative disposizioni del RGPD e coerentemente con le previsioni contenute in apposite linee guida approvate dall'Ufficio di presidenza.

Art. 411 ter

(Responsabile della protezione dei dati personali)

1. Il responsabile della protezione dei dati personali (RPD) è nominato, previo atto di indirizzo formulato dall'Ufficio di presidenza, con apposito provvedimento del Segretario generale, secondo le modalità stabilite dall'articolo 37 del RGPD.

2. Il RPD provvede a svolgere i compiti di cui all'articolo 39 del RGPD nonché quelli ulteriori stabiliti con il provvedimento di nomina o con atto successivo, da eseguirsi nei termini e con le modalità di cui all'articolo 38 dello stesso.

Art. 411 quater

(Gruppo di Lavoro Privacy)

1. È istituito il Gruppo di Lavoro Privacy, di seguito denominato Gruppo di lavoro.

2. Il Gruppo di lavoro, costituito con apposito provvedimento del Segretario generale, è preposto allo svolgimento di compiti operativi di analisi, gestione e soluzione dei problemi applicativi del RGPD nonché all'individuazione di soluzioni tecniche tese a prevenire e contrastare i rischi connessi alla sicurezza informatica correlati alla protezione dei dati personali.

3. I componenti del Gruppo di lavoro, scelti tra i dipendenti in servizio presso il Consiglio regionale o altre pubbliche amministrazioni ovvero tra soggetti esterni all'amministrazione, devono possedere, in ragione della intersettorialità, interdisciplinarietà e integrazione funzionale dei compiti che lo stesso è chiamato a svolgere, specifiche competenze e professionalità in materia di protezione dei dati personali."

7. Gli articoli 412, 413, 414, 415, 416 e 417 sono abrogati.

8. L'articolo 418 è sostituito dal seguente:

"**Art. 418**

(Affidamento in esterno di attività di trattamento dei dati personali. Responsabili esterni del trattamento)

1. Il Titolare, ai sensi dell'articolo 28 del RGPD e nel rispetto della normativa in materia di contratti pubblici, può affidare il trattamento dei dati personali a soggetti terzi prestatori di servizi, denominati Responsabili esterni del trattamento, che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento stesso soddisfi i requisiti del RGPD medesimo e garantisca la tutela dei diritti dell'interessato.

2. I Responsabili esterni del trattamento assumono le stesse funzioni dei Delegati, sottoscrivendo un contratto di prestazione di servizi che li obbliga all'osservanza delle prescrizioni disposte dal RGPD.".

9. Dopo l'articolo 418 è inserito il seguente:

"**Art. 418 bis**

(Registri delle attività di trattamento e delle violazioni dei dati personali)

1. Il Segretario generale, con proprio provvedimento, in conformità con quanto previsto dagli articoli 30 e 33, paragrafo 5. del RGPD, istituisce rispettivamente il registro delle attività di trattamento dei dati personali e il registro delle violazioni dei dati personali, che sono tenuti, sia in formato cartaceo che in formato elettronico, dalla struttura organizzativa competente in materia di tutela della *privacy.*

2. I registri di cui al comma 1 sono aggiornati e implementati dai Delegati, ognuno per la parte di propria competenza, secondo i termini e le modalità stabiliti con proprio atto dal Segretario generale.".

10. Gli articoli 419, 420, 421, 422, 423 e 424 sono abrogati.

11. L'articolo 425 è sostituito dal seguente:

"**Art. 425**

(Informazioni e comunicazioni per l'esercizio dei diritti dell'interessato)

1. Il Titolare, ai sensi dell'articolo 12 del RGPD, adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14, le comunicazioni tese ad agevolare l'esercizio dei diritti di cui agli articoli 15, 16, 17, 18, 20, 21 e 22 e le comunicazioni previste dagli articoli 19 e 34 del medesimo RGPD.

2. Le informazioni e le comunicazioni di cui al comma 1 sono fornite per iscritto. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

3. Le informazioni e le comunicazioni di cui al comma 1 sono gratuite, salvo quanto previsto dal paragrafo 5. dell'articolo 12 del RGPD.".

12. L'articolo 426 è sostituito dal seguente:

"**Art. 426**
(*Diritti dell'interessato. Modalità di esercizio*)

1. L'interessato esercita i diritti di accesso, rettifica, cancellazione o anonimato, limitazione e opposizione di trattamento nonché di portabilità di dati secondo quanto previsto dagli articoli da 15 a 22 del RGPD.

2. I diritti di cui al comma 1 sono esercitati con richiesta rivolta al Titolare o ai singoli Delegati, anche per il tramite di una Persona autorizzata al trattamento dei dati personali, a cui deve essere fornito idoneo riscontro senza ritardo. Tale richiesta è presentata dall'interessato, anche attraverso l'utilizzo degli appositi moduli pubblicati sul sito web del Consiglio regionale, corredata da un relativo documento di riconoscimento in corso di validità, con una delle seguenti modalità:

a) a mezzo di raccomandata con ricevuta di ritorno;

b) per via telematica, ai sensi dell'articolo 65 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) e successive modifiche;

c) mediante consegna a mano all'ufficio accettazione corrispondenza del Consiglio regionale.

3. I singoli Delegati forniscono all'interessato, secondo le modalità e i termini previsti dall'articolo 12 del RGPD, le informazioni relative allo stato della procedura concernente la richiesta presentata.".

13. Dopo l'articolo 426 è inserito il seguente:

"**Art. 426 bis**
(*Mezzi di ricorso*)

1. Qualora l'interessato ritenga che i diritti di cui gode a norma del RGPD siano stati violati a seguito di un trattamento, può attivare le forme di tutela previste dal Capo VIII del medesimo.".

14. Gli articoli 427 e 428 sono abrogati.

15. L'articolo 429 è sostituito dal seguente:

"Art. 429
(*Sicurezza dei dati e dei sistemi)*

1. La sicurezza dei dati e dei sistemi avviene nel rispetto di quanto previsto dalla sezione 2 del Capo IV del RGPD e, in particolare, dall'articolo 32 dello stesso.".

16. Gli articoli 430 e 431 sono abrogati.

17. L'articolo 432 è sostituito dal seguente:

"**Art. 432**

(Disposizioni finali)

1. Per quanto non previsto dalle disposizioni del presente Capo si applicano le norme del RGPD e del Codice.".

Allegato B alla deliberazione dell'Ufficio di presidenza 12 giugno 2018, n. 60

Linee guida per il trattamento dei dati personali

Si riportano in appresso, a completamento delle modifiche al regolamento di organizzazione del Consiglio regionale concernenti la rivisitazione dell'assetto organizzativo privacy alla luce delle novità introdotte dal regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, per il seguito denominato RGPD, le linee guida per il trattamento dei dati personali.
Preliminarmente viene di seguito illustrato, ai fini di una più agevole comprensione dei contenuti del presente documento, l'assetto organizzativo *privacy* del Consiglio regionale, che si articola in:

a) "Titolare del trattamento" - ossia il soggetto che determina le finalità e i mezzi del trattamento dei dati personali effettuati dalle diverse strutture organizzative del Consiglio regionale - è lo stesso Consiglio regionale;
b) "Delegati al trattamento" - ossia coloro che effettuano qualsiasi operazione od insieme di operazioni, compiuto con o senza l'ausilio di processi di automazione e applicate ai dati personali o insiemi di dati personali - per il seguito Delegati, sono i dirigenti e i titolari di incarichi di funzione dirigenziale, comunque denominati, che comportano l'esercizio delle competenze di amministrazione e gestione, ciascuno per la parte di propria competenza. Tale determinazione tiene conto, in particolare, della complessità e della molteplicità delle funzioni istituzionali del Consiglio regionale in cui, ovviamente, le attività di gestione finanziaria, tecnica e amministrativa, compresa la competenza a stipulare contratti, rientrano tra le specifiche funzioni dirigenziali. I dirigenti e i titolari di incarichi di funzione dirigenziale, comunque denominati, chiamati a dare attuazione alle direttive e agli indirizzi del competente organo politico, hanno, in ragione del ruolo svolto, una sicura centralità nel trattamento dei dati personali. Relativamente alle strutture di diretta collaborazione degli organi istituzionali, degli organi di controllo e garanzia e degli organi politici di cui all'articolo 3 del regolamento di organizzazione del Consiglio regionale, i rispettivi Delegati sono individuati dalle pertinenti disposizioni dello stesso;
c) "Persone autorizzate al trattamento", sono i dipendenti formalmente autorizzati al trattamento di dati personali dai Delegati, con specifica individuazione dell'ambito del trattamento consentito, sul presupposto dell'assegnazione alla relativa struttura organizzativa;
d) "Responsabili esterni del trattamento", sono i soggetti terzi prestatori di servizi, scelti dal Titolare del trattamento ai sensi dell'articolo 28 del RGPD e nel rispetto della normativa in materia di contratti pubblici, che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti dello stesso RGPD e garantisca la tutela dei diritti dell'Interessato. Essi assumono le stesse funzioni dei Delegati, sottoscrivendo un contratto di prestazione di servizi che li obbliga all'osservanza delle prescrizioni disposte dal RGPD;

e) "Responsabile della protezione dei dati personali (RPD)", è il soggetto (persona fisica o giuridica) chiamato a svolgere i compiti e le attività previsti dall'articolo 39 del RGPD nonché quelli ulteriori stabiliti con il provvedimento di nomina o con atto successivo, da eseguirsi nei termini e con le modalità di cui all'articolo 38 dello stesso;
f) "Gruppo di Lavoro Privacy", è un organismo, costituito con apposito provvedimento del Segretario generale, preposto allo svolgimento di compiti operativi di analisi, gestione e soluzione dei problemi applicativi del RGPD nonché all'individuazione di soluzioni tecniche tese a prevenire e contrastare i rischi connessi alla sicurezza informatica correlati alla protezione dei dati personali. I suoi componenti, scelti tra i dipendenti in servizio presso il Consiglio regionale o altre pubbliche amministrazioni ovvero tra soggetti esterni all'amministrazione, in ragione della intersettorialità, interdisciplinarietà e integrazione funzionale dei compiti che lo stesso è chiamato a svolgere, che interessano trasversalmente tutte le strutture in cui si declina l'organizzazione del Consiglio regionale, devono possedere specifiche competenze e professionalità in materia di protezione dei dati personali.

1. Compiti del Delegato

Il Delegato, al fine di poter efficacemente adempiere alle proprie funzioni, si avvale della collaborazione delle Persone autorizzate al trattamento.
Il Delegato, in particolare, svolge i seguenti compiti:

- **verifica del trattamento dei dati**: tale attività implica che lo stesso debba osservare i principi applicabili al trattamento dei dati e le condizioni di liceità dello stesso, garantire la qualità dei dati personali, le corrette modalità di raccolta, conservazione e trattamento in generale degli stessi secondo quanto disposto dal RGPD, anche da parte delle Persone autorizzate al trattamento, nonché vigilare sul rispetto delle istruzioni impartite alle stesse;
- **documentazione delle scelte**: tale attività comporta che lo stesso debba tenere traccia del percorso logico e delle motivazioni che hanno condotto ad effettuare le scelte in ambito *privacy*;
- **informative**: tale attività implica lo svolgimento, a favore dell'Interessato, di quanto previsto dalle disposizioni di cui al Capo III del RGPD;
- **aggiornamento e implementazione del registro delle attività di trattamento e di quello delle violazioni dei dati personali (c.d. registro dei databreach)**;
- **valutazione dell'impatto sulla protezione dei dati e la consultazione preventiva ex articoli 35 e 36 del RGPD**;
- **attuazione e valutazione delle misure di sicurezza dei dati e dei sistemi secondo quanto previsto dalla Sezione 2, del Capo IV del RGPD**;
- **cura dei rapporti con il RPD:** tale attività comporta un tempestivo e adeguato coinvolgimento del RPD in tutte le questioni riguardanti la protezione dei dati personali;

— **adozione delle misure indicate nei paragrafi 5 e 6 del presente documento, in caso di violazione dei dati personali**.

2. I registri delle attività di trattamento e delle violazioni dei dati personali (c.d. registro dei databreach)

2.1 Registro delle attività di trattamento dei dati personali.

L'articolo 30, paragrafo 1. del RGPD prevede l'obbligo di tenere un registro delle attività di trattamento dei dati personali. Tale registro è tenuto, sia in formato cartaceo che in formato elettronico, dalla struttura organizzativa competente in materia di tutela della *privacy* e si configura come:

— un "cruscotto informativo", in merito al rispetto degli adempimenti previsti dal RGPD;

— un "gestionale", che consente di monitorare costantemente la situazione relativamente al trattamento dei dati personali;

— uno strumento correlato all'analisi dei rischi per i diritti e le libertà delle persone fisiche, connessi al trattamento dei dati personali.

Il registro deve contenere le informazioni relative al trattamento dei dati personali di cui al richiamato articolo del RGPD.

Esso è aggiornato e implementato dai Delegati, ognuno per la parte di propria competenza, secondo i termini e le modalità stabiliti con proprio atto dal Segretario generale, che provvede anche all'istituzione dello stesso.

2.2. Registro delle violazioni dei dati personali (c.d. registro dei *databreach*)

L'articolo 33, paragrafo 5. del RGPD prevede l'obbligo di tenere un registro delle violazioni dei dati personali, che documenti le circostanze, le conseguenze e i provvedimenti adottati per porre rimedio alle violazioni medesime. Tale registro consente all'Autorità di controllo di verificare l'osservanza delle previsioni di cui allo stesso articolo 33.

Al registro in questione si applica quanto previsto al sub-paragrafo 2.1, con riferimento alla istituzione, alla tenuta, all'aggiornamento e all'implementazione.

3. Sicurezza

3.1 Introduzione

I dati personali, siano essi in formato digitale che su sopporto cartaceo, devono essere custoditi con cura al fine di preservarne le caratteristiche di integrità, disponibilità e confidenzialità e in modo da garantire un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato di essi e delle attrezzature impiegate per il trattamento.

Il principio di "responsabilizzazione" ("*accountability*") impone di mettere in atto *"misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento."* (articolo 24, paragrafo 1. del RGPD). Tra queste misure ve ne sono alcune rilevanti quali *"la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a*

integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati." (articolo 25, paragrafo 1. del RGPD).
In ragione del fatto che i trattamenti possono essere effettuati con o senza l'ausilio di strumenti elettronici, le misure di sicurezza da adottare devono essere differenti e adeguate alle diverse situazioni e alla natura dei dati trattati. Rientra in ogni caso tra i compiti del Delegato l'adozione di ulteriori e più adeguate misure di sicurezza, ritenute necessarie per la particolare tipologia dei dati trattati presso la propria struttura.

3.2 Censimento del patrimonio informativo

I Delegati e le Persone autorizzate al trattamento devono conoscere ed essere consapevoli della natura e della delicatezza dei dati personali trattati. La conoscenza di questi elementi è propedeutica a qualsiasi valutazione dei rischi sui dati trattati e alla conseguente individuazione delle contromisure da adottare. In tale ottica, il Registro delle attività di trattamento sopra descritto ha la funzione, tra le altre, di raccogliere e dare evidenza agli elementi sopra indicati.

3.3 Analisi dei rischi

Il RGPD introduce il problema dei rischi nel Considerando (75), che si riporta di seguito:
"*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati generici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.*".
Il successivo Considerando (76) aggiunge che "*La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*".
Da quanto sopra indicato risulta chiara l'importanza della individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio.

4. Valutazione d'impatto

La valutazione d'impatto è disciplinata dall'articolo 35 del RGPD e per essa, può essere richiesta, da parte dei Delegati, la collaborazione del RDP sotto forma di parere (articolo 39, paragrafo 1., lettera c)).
Il paragrafo 3. dell'articolo 35 del RGPD, precisa che la valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:
"

a) *una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
b) *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;*
c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*".

La valutazione d'impatto è, altresì, richiesta nei casi che saranno indicati dall'Autorità di controllo in un apposito elenco e, comunque, ogni qualvolta *"l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche."* (articolo 35, paragrafi 1. e 4. del RGPD).

5. Violazione dei dati personali (databreach)

Per la violazione dei dati personali ossia per una violazione di sicurezza che comporta *"accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"* (articolo 4, paragrafo 1., n. 12) del RGPD), il RGPD stabilisce all'articolo 33, paragrafo 1. che *"..... il titolare del trattamento notifica la violazione all'autorità di controllo competente ... senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*"
Si intendono oggetto dell'eventuale obbligo di notifica, di cui sopra, anche i *databreach* avvenuti presso Responsabili esterni del trattamento.
Ogni Delegato, per quanto di sua competenza, non appena venuto a conoscenza di un *databreach*, procede, entro 72 ore dalla scoperta, in luogo del Titolare, a:

- effettuare una prima necessaria istruttoria e valutazione dei rischi per i diritti e le libertà dell'Interessato e ad avvisare tempestivamente la struttura competente in materia di tutela della privacy e il RDP;
- a notificare, fatta eccezione per i casi in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, all'Autorità di controllo lo stesso *databreach*.

Il paragrafo 3. dell'articolo 35 specifica che la notifica in parola deve almeno:
"

a) *descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione*;
b) *comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*
c) *descrivere le probabili conseguenze della violazione dei dati personali;*
d) *descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*".

Tutte le Persone autorizzate al trattamento devono essere adeguatamente istruite affinché trattino correttamente i dati personali e informino, con la massima celerità, il Delegato di ogni violazione rilevata, affinché quest'ultimo possa procedere nei termini e con le modalità di cui sopra.

6. Comunicazione di databreach all'Interessato

L'articolo 34 del RGPD disciplina la comunicazione all'Interessato dell'avvenuto *databreach*. Tale comunicazione è obbligatoria quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche e deve essere effettuata, al ricorrere di tali condizioni, senza ingiustificato ritardo.
Ci sono, tuttavia, delle eccezioni a tale obbligo di comunicazione, disciplinate dall'articolo 34, paragrafo 3. del RGPD ossia quando:
"

a) *il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;*
b) *il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;*
c) *detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.*".

Il Delegato verifica la sussistenza o meno delle condizioni che dispensano dall'obbligo di comunicazione in parola, con la consulenza del RDP e l'assistenza delle strutture competenti in materia di tutela della privacy e di informatica. Procede quindi, se del caso, a comunicare la violazione all'Interessato. La determinazione, in un senso o nell'altro, del Delegato rispetto alla comunicazione in parola deve comunque essere motivata.