MODELLO ORGANIZZATIVO PRIVACY PER I TRATTAMENTI DEI DATI PERSONALI DI TITOLARITÀ DEL CONSIGLIO REGIONALE DEL FRIULI VENEZIA GIULIA AI SENSI DEL REGOLAMENTO (UE) 2016/679 e DEL CODICE PRIVACY (D.lgs 196/2003 e s.m.i.)

ACRONIMI E DEFINIZIONI

GDPR	Regolamento Generale sulla Protezione dei dati Personali - General Data Protection Regulation (Regolamento UE 2016/679)
CODICE PRIVACY	Il "Codice in materia di protezione dei dati personali" del 30 giugno 2003 n. 196, detto anche "Testo unico sulla privacy", entrato in vigore il primo gennaio 2004, contiene le norme nazionali relative alla tutela dei dati personali. È stato integrato ed aggiornato dal D.lgs. del 10 agosto 2018, n. 101, che recepisce le modifiche introdotte con l'entrata in vigore, il 25 maggio 2018, del GDPR UE 2016/679.
Garante Privacy	Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente, istituita dalla cosiddetta "Legge sulla privacy". È l'autorità di controllo designata ai fini dell'attuazione del Regolamento Generale sulla Protezione dei Dati Personali UE 2016/679 (art. 15).
RPD/DPO(Data Protection Officer)	Soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali
Anonimizzazione	È la trasformazione irreversibile dei dati personali che fa sì che le persone fisiche interessate non possano essere più identificate.
Indicizzazione	L'indicizzazione non elimina definitivamente il dato, ma lo rende non direttamente accessibile tramite motori di ricerca esterni all'archivio in cui quel contenuto si trova.
Pseudonimizzazione	Trattamento dei dati personali che prevede l'oscuramento o la sostituzione parziale dei dati personali di un soggetto in modo da impedirne l'identificazione senza l'utilizzo di informazioni aggiuntive.
Informativa	Nota con la quale la pubblica amministrazione informa i cittadini, i destinatari e tutti i potenziali interessati sulla modalità del trattamento dei dati e sull'applicazione di quanto previsto dalla normativa vigente in materia di privacy, sulle procedure attuate dall'ente titolare dei dati, sulla loro protezione e sicurezza e sulla finalità degli stessi. È resa ai sensi degli articoli 13 e 14 del GDPR.
Base giuridica del trattamento	È ciò che autorizza legalmente il trattamento dei dati. Il titolare del trattamento deve rispettare le condizioni previste dall'art. 6 del GDPR ed essere sempre in grado di dimostrare la correttezza della scelta effettuata. Deve essere indicata nell'informativa rivolta agli utenti.
Interessato	Persona fisica alla quale si riferiscono i dati raccolti o in trattamento (articolo 4, paragrafo 1, punto 1 del GDPR).
Contitolare del	Si parla di contitolarità quando due o più titolari determinano congiuntamente

trattamento	"perché" e "come" debbano essere trattati i dati personali.
Privacy by design	Criterio che richiede che il titolare del trattamento dei dati personali adotti misure tecniche e organizzative idonee sin dal momento della progettazione del trattamento dei dati personali.
Privacy by default	Criterio che presuppone misure che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.
DPIA (Data privacy impact assestment)	Quando un determinato trattamento, tenuto conto dell'uso di nuove tecnologie e della sua natura, del contesto e delle finalità, può presentare un rischio elevato per i diritti e la libertà delle persone fisiche, il titolare, nei casi espressamente previsti dal GDPR, deve effettuare una valutazione dei rischi connessi al trattamento di dati con l'obiettivo di identificare le misure più idonee per affrontarli.
Violazione dei dati personali (o Data Breach)	La 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.
Registro delle attività di trattamento	Documento redatto dal titolare e dal responsabile in forma cartacea o elettronica, disciplinato dall'art. 30 del GDPR, in cui sono indicate le caratteristiche, le modalità e le finalità dei trattamenti effettuati.
Registro violazioni	Registro che documenta gli incidenti che comportano una violazione dei dati personali (art. (art.33, p.5 GDPR).

PREMESSE

Il quadro normativo che regola la protezione dei dati personali è delineato principalmente dal Regolamento (UE) 2016/679, noto come Regolamento Generale sulla Protezione dei Dati (GDPR), e dalle disposizioni del decreto legislativo 30 giugno 2003, n. 196, meglio conosciuto come Codice della privacy, il quale è stato aggiornato con il d.lgs. n. 101/2018 per allinearsi alle prescrizioni del GDPR.

In particolare i principi fondamentali applicabili al trattamento di dati personali sono indicati nell'Art. 5 del GDPR (Regolamento generale 2016/679/UE) e sono i seguenti:

1. **liceità, correttezza e trasparenza** - i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
2. **limitazione della finalità** - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali;
3. **minimizzazione dei dati** - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **esattezza** - esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
5. **limitazione della conservazione** - conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato;
6. **integrità e riservatezza** - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
7. **responsabilizzazione (accountability):** sancisce in capo al titolare del trattamento e delegati, il principio di "responsabilizzazione" che si compone di tre elementi essenziali: trasparenza, responsabilità e conformità.

Il GDPR stabilisce un dettagliato insieme di regole per la protezione dei dati personali, definendo i ruoli e le responsabilità delle varie figure coinvolte nel loro trattamento.

Tra i principali soggetti identificati dalla normativa, troviamo:

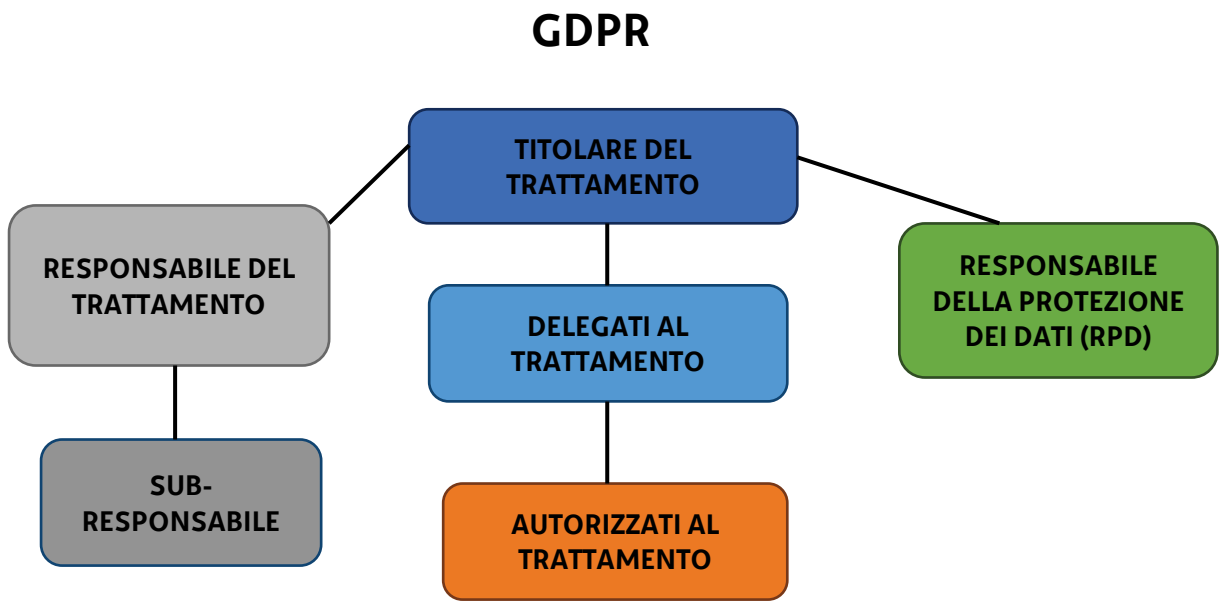
- Il Titolare del trattamento, che ai sensi dell'Art. 4, par. 1, n. 7 e dell'art. 24 del GDPR, nonché dei Considerando 74 e 78, è colui che determina le finalità e i mezzi del trattamento dei dati personali.
- Il Responsabile della Protezione dei dati (RPD o DPO, Data Protection Officer), le cui funzioni sono descritte dagli Artt. 37 e seguenti del GDPR e dal Considerando 97, è incaricato di monitorare la conformità alle norme sulla protezione dei dati, fornire consulenza e fungere da punto di contatto con l'autorità di controllo.
- I Responsabili del trattamento, come indicato dall'Art. 4, par. 1, n. 8 e dall'art. 28 del GDPR, e dal Considerando 81, sono soggetti che trattano dati personali per conto del titolare.

- I Delegati del Titolare, introdotti dall'Art. 2 quaterdecies, comma 1, del Codice Privacy, sono i soggetti che trattano dati "per conto" e sotto la diretta autorità del Titolare.
- Gli Autorizzati al trattamento, definiti dall'Art. 4, par. 10, dall'articolo 29 e dall'articolo 32, par. 4 del GDPR, nonché dall'art. 2 quaterdecies, comma 2, del Codice Privacy, sono i soggetti incaricati che trattano i dati personali sotto l'autorità diretta del Titolare o del Responsabile.

In particolare, Il GDPR, nel riformare il precedente impianto normativo in materia di protezione dei dati, ha inserito l'innovativo principio di Accountability (o "Responsabilizzazione") del Titolare, di eventuali Contitolari e dei Responsabili del trattamento, nell'adozione di misure tecniche ed organizzative adeguate ed efficaci, con l'onere di dimostrare la conformità delle attività di trattamento al GDPR stesso, nonché mettendo in atto procedure per riesaminare e aggiornare le misure stesse.

Il Titolare del trattamento è chiamato a rimodulare i processi di gestione dei dati personali secondo i principi di Data Protection "by design" e "by default", per avere la certezza che le misure tecniche e organizzative siano adottate ed integrate fin dalla progettazione (ideazione) del trattamento, siano rivolti a valutare i rischi di minacce che possono generare violazioni dei dati personali, siano stabiliti a priori gli interventi, per avere la garanzia della liceità del trattamento, siano indirizzate a rendere i collaboratori, nella qualità di soggetti autorizzati, consapevoli del valore del dato attraverso la formazione e la corretta applicazione di istruzioni ad hoc.

Diventa, quindi, prioritaria l'organizzazione dell'ente al fine di definire i compiti e le responsabilità dei soggetti coinvolti nel trattamento dei dati personali in base alla seguente **architettura dei ruoli previsti dal GDPR.**



È essenziale identificare con precisione i soggetti che ricoprono i ruoli sopra menzionati all'interno del Consiglio regionale Fvg.

Scopo del presente documento è quindi definire il modello organizzativo della struttura amministrativa del Consiglio regionale del Friuli Venezia Giulia in conformità con il Regolamento europeo 2016/679 denominato GDPR e con il Codice privacy (d. lgs. 196/2003 e D.lgs. 101/2018).

Nello specifico, consiste nel prendere in esame i ruoli e le responsabilità previsti dal GDPR e descrivere l'assetto organizzativo del Consiglio regionale in materia di privacy al fine di garantire nel trattamento dei dati personali la tutela dei diritti di libertà delle persone, e quindi:

a) Identificare il Titolare del trattamento dei dati personali del Consiglio regionale FVG;

b) Descrivere i compiti assegnati al Responsabile della Protezione dei dati;

c) Individuare i ruoli e le responsabilità assegnate ai Delegati e autorizzati dal Titolare a vari livelli, (dirigenti e dipendenti), al fine di garantire la corretta gestione dei dati in conformità alla normativa di riferimento;

d) Definire i Responsabili del trattamento esterni;

e) Prevedere i Referenti privacy all'interno dell'Organizzazione consiliare;

f) Disposizioni per il personale dei gruppi consiliari.

Tale documento viene portato a conoscenza di tutti i dirigenti, funzionari, collaboratori, dipendenti e tirocinanti che svolgono la propria attività all'interno del Consiglio regionale mediante la pubblicazione nella intranet consiliare nonché attraverso attività di sensibilizzazione e formazione in materia di protezione dei dati personali.

A tale documento di definizione del modello organizzativo seguiranno le linee guida e dettagliate informazioni per l'attuazione degli ulteriori obblighi derivanti dal GDPR.

1. TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento, come definito dall'articolo 4, paragrafo 1, numero 7 del Regolamento Generale sulla Protezione dei Dati (GDPR), è la figura centrale che determina le finalità e i mezzi del trattamento dei dati personali. Può trattarsi di una persona fisica o giuridica, di un'autorità pubblica, di un servizio o di un altro organismo che agisce da solo o congiuntamente ad altri.

Il Titolare del trattamento ha la responsabilità complessiva di assicurare che ogni trattamento di dati personali, sia quello svolto direttamente sia quello effettuato per suo conto da terzi, sia conforme alle disposizioni del GDPR, come sottolineato dal Considerando 74 del Regolamento.

In particolare, l'articolo 24 del GDPR impone al Titolare del trattamento di adottare misure tecniche e organizzative adeguate per garantire e dimostrare che il trattamento è conforme al Regolamento, considerando la natura, l'ambito, il contesto e le finalità del trattamento, nonché i rischi per i diritti e le libertà degli individui e aggiornare tali misure quando necessario.

Quando due o più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento di dati personali si dicono Contitolari (art 26 GDPR). I Contitolari devono definire tramite accordo trasparente ruoli e ripartizione delle responsabilità e degli obblighi derivati dal GDPR.

Le responsabilità del Titolare del trattamento includono:

a) Assicurare e dimostrare il rispetto dei principi di trattamento dei dati personali, come l'articolo 5, paragrafo 2 del GDPR richiede, tra cui liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, garantire che le finalità dei trattamenti siano sempre determinate, esplicite e legittime e che i dati raccolti siano adeguati, pertinenti, esatti ed aggiornati, oltre che limitati a quanto necessario rispetto alle finalità;
b) Implementare le disposizioni normative necessarie, in linea con le modifiche introdotte dal Codice per la protezione dei dati personali (D.lgs. 196/2003, come modificato dal D.lgs. n. 101/2018), per adeguarsi al GDPR;
c) Designare il Responsabile della Protezione dei Dati (RPD o DPO), figura prevista dagli articoli 37 e seguenti del GDPR, che ha il compito di monitorare la conformità alle norme sulla protezione dei dati, fornire consulenza e agire come punto di contatto con l'autorità di controllo;
d) Designare, ai sensi dell'articolo 2 quaterdecies comma 1 del Codice della privacy, i soggetti delegati a specifici compiti e funzioni legati al trattamento dei dati personali, operanti sotto la sua autorità diretta;
e) Stabilire, come previsto dall'articolo 2 quaterdecies comma 2 del Codice della privacy, le modalità più opportune per autorizzare al trattamento dei dati personali, le persone che operano sotto la propria autorità diretta;
f) Condurre, attraverso i servizi competenti, controlli sull'osservanza delle normative vigenti in materia di trattamento dei dati, in collaborazione con il RPD;
g) Organizzare attività formative per i dipendenti e i collaboratori del Consiglio regionale FVG, al fine di promuovere la consapevolezza e la comprensione delle norme relative alla protezione dei dati personali.

Il Consiglio regionale del Friuli Venezia Giulia, in qualità di autorità pubblica, è il titolare del trattamento dei dati personali, e nello specifico:

1. L' Assemblea Legislativa:
    - nel redigere gli atti normativi, ove necessario, disciplina il trattamento dei dati personali afferenti la propria competenza nel rispetto degli obblighi derivanti dal Codice privacy e dal GDPR;

- approva con delibera del Consiglio Regionale il proprio Regolamento interno per il funzionamento dell'attività consiliare (legislativa, di controllo etc.) e ne cura le modifiche se necessario anche in considerazione della normativa sulla protezione dei dati personali;

2. L' Ufficio di Presidenza:

   - Approva il Regolamento di organizzazione degli Uffici del Consiglio regionale;
   - Nomina RPD/DPO, definisce i compiti specifici e assegna le risorse per funzionamento;
   - Approva gli schemi di accordo di Contitolarità e con i Responsabili del trattamento esterni, definendone i compiti e le responsabilità (Art. 26 GDPR);
   - Designa i soggetti delegati e autorizzati al trattamento dei dati personali, operanti sotto la sua autorità diretta;
   - Adotta Linee Guida per la notifica delle violazioni di dati personali (GDPR Art. 33) c.d.data breach nell'ambito del Consiglio regionale.

2. IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD/DPO)

Il Responsabile della Protezione dei Dati (RPD), noto anche come Data Protection Officer (DPO), è una figura chiave nel quadro normativo del Regolamento (UE) 2016/679 (GDPR).

Nell'ambito del Consiglio regionale, il RPD è individuato all'interno della Segreteria generale ed è nominato con delibera dell'Ufficio di Presidenza, deve riferire al Segretario Generale in quanto vertice gerarchico del Titolare del trattamento.

Il RPD, svolge un ruolo fondamentale nell'assicurare che il Consiglio regionale operi in conformità con le normative sulla protezione dei dati, fungendo da garante per i diritti degli interessati e come punto di riferimento per tutte le questioni relative alla privacy e al trattamento dei dati personali, i suoi compiti e funzioni discendono direttamente dalla normativa europea (art. 39 GDPR).

Tra i compiti principali del RPD vi sono:

a) Informazione e consulenza: Il RPD ha il dovere di informare e fornire consulenza al Titolare del trattamento, ai delegati e ai dipendenti coinvolti nel trattamento dei dati personali riguardo agli obblighi imposti dal GDPR e da altre disposizioni di legge nazionali o dell'Unione europea in materia di protezione dei dati.

b) Monitoraggio della conformità: Il RPD sorveglia sull'osservanza del GDPR, delle altre disposizioni normative nonché delle linee guida relative alla protezione dei dati personali adottate all'interno del Consiglio regionale.

c) Valutazione d'impatto sulla protezione dei dati (DPIA): Il RPD deve fornire un parere, qualora richiesto, in merito alla valutazione d'impatto sulla protezione dei dati personali, come previsto dall'articolo 35 del GDPR. Inoltre, è suo compito sorvegliare lo svolgimento della DPIA da parte del delegato competente, assicurandosi che venga condotta correttamente e che i risultati siano presi in considerazione nel processo decisionale relativo al trattamento dei dati.

d) Punto di contatto per gli interessati: Il RPD agisce come punto di contatto per gli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti garantiti dal RGPD.

e) Cooperazione con l'Autorità Garante: Il RPD deve cooperare attivamente con l'Autorità Garante per la protezione dei dati personali, l'ente preposto a vigilare sull'applicazione della normativa sulla privacy in Italia.

f) Punto di contatto con l'Autorità Garante: Il RPD funge da punto di contatto tra il Consiglio regionale e l'Autorità Garante per tutte le questioni connesse al trattamento dei dati personali, inclusa la consultazione preventiva di cui all'articolo 36 del GDPR. Il RPD può anche svolgere consultazioni su altre questioni rilevanti per la protezione dei dati.

g) Registro dei trattamenti: Il RPD con l'Ufficio privacy e il Segretario generale coordina e fornisce indirizzi per l'aggiornamento e la tenuta del Registro dei trattamenti del Consiglio regionale, uno strumento essenziale per documentare tutte le attività di trattamento dei dati personali svolte e per dimostrare la conformità al GDPR.

h) Registro delle violazioni: Il RPD con l'Ufficio privacy e il Segretario generale coordina e fornisce indirizzi per documentare qualsiasi violazione dei dati personali, comprese le circostanze della violazione, le sue conseguenze e le misure adottate per rimediare.

i) Rappresentanza istituzionale: Il RPD rappresenta il Consiglio regionale all'interno del gruppo di lavoro in ambito Privacy della Conferenza delle Assemblee legislative, contribuendo così alla definizione delle linee guida e delle strategie in materia di protezione dei dati a livello di Assemblee Legislative nazionali.

j) Coordinamento dei referenti privacy: Il RPD, con l'ufficio privacy e il Segretario generale, coordina il Gruppo dei referenti privacy, assicurando che vi sia una comunicazione efficace e una collaborazione tra le varie strutture del Consiglio regionale in materia di protezione dei dati.

3.DELEGATI DEL TITOLARE

Il Titolare del trattamento, ai sensi dell'articolo 2 quaterdecies, comma 1 del Codice Privacy, ha la facoltà di delegare specifici compiti e funzioni in materia di trattamento dei dati personali a persone fisiche designate all'interno dell'organizzazione. Queste persone, che operano sotto l'autorità del Titolare, assumono la responsabilità di assicurare il rispetto degli obblighi previsti dal GDPR e dalla normativa nazionale in materia di protezione dei dati personali.

In caso di trattamenti trasversali tra più Strutture, si applica il criterio della prevalenza della competenza per materia.

Nell'ambito del Consiglio regionale, il Titolare del trattamento dei dati personali, per l'esercizio delle sue funzioni, si avvale delle seguenti figure di delegati:

- **il Segretario Generale**
- **il Vicesegretario generale**
- **il Capo di Gabinetto**
- **i Dirigenti, il Direttore responsabile dell'Agenzia Consiglio Notizie e il Portavoce, per i propri ambiti di competenza individuati nelle rispettive declaratorie di funzioni.**

il Segretario Generale:

Rappresenta il vertice gerarchico del Titolare del trattamento e, in quanto tale, è tenuto a:

1. Assicurare che i trattamenti di dati personali all'interno del Consiglio regionale siano effettuati nel rispetto dei principi fondamentali del GDPR, come la liceità, la correttezza, la trasparenza, la limitazione della finalità, la minimizzazione dei dati, l'esattezza, la limitazione della conservazione, l'integrità e la riservatezza.
2. Adottare le necessarie soluzioni di *privacy by design* e *privacy by default* implementando in collaborazione con il RPD e Delegati, le misure tecniche e organizzative che minimizzino la

raccolta di dati personali, limitando il loro trattamento ai soli scopi necessari e proteggendo i dati contro accessi non autorizzati, distruzione o perdite (art. 25 GDPR).

3. Fornire formazione e aggiornamento continuo al personale che opera all'interno del Consiglio regionale, per assicurare che sia a conoscenza delle procedure e delle disposizioni in materia e per sensibilizzarlo sulle questioni relative alla protezione dei dati personali.
4. Monitorare la conformità dei trattamenti di dati personali alle normative vigenti effettuando attraverso i servizi competenti, apposite verifiche sulle modalità dei trattamenti in collaborazione con il RPD e l'Ufficio privacy.
5. stipulare, negli ambiti di propria competenza, contratti con i Contitolari e Responsabili del trattamento esterni, conformi all'articolo 28, comma 3 del GDPR al fine di garantire che i soggetti terzi che trattano dati per conto del Consiglio regionale, operino in maniera conforme alle istruzioni ricevute e alle normative vigenti. Il contratto deve dettagliare specificamente gli obblighi del responsabile del trattamento, comprese le misure di sicurezza da adottare e le procedure in caso di violazione dei dati.
6. Collaborare con il RPD e con le autorità di controllo, fornendo tutte le informazioni necessarie e partecipando attivamente alla risoluzione di eventuali problemi relativi alla protezione dei dati personali.
7. Adotta Linee Guida in materia di trattamento e sicurezza per la protezione di dati personali, previo parere del RPD, cui devono attenersi, nello svolgimento della propria attività coloro che trattano dati personali nell'ambito del Consiglio regionale (GDPR Art. 32).
8. Adottare con proprio decreto il Registro dei trattamenti dei dati personali (art. 30 GDPR) e il Registro delle violazioni (art.33, p.5 GDPR).
9. In caso di violazione dei dati personali *(data breach)*, il Segretario generale è responsabile di notificare l'incidente all'Autorità Garante per la protezione dei dati personali ed eventualmente agli interessati a nome del Titolare del trattamento, secondo quanto previsto dagli articoli 33 e 34 del GDPR.
10. Al Segretario generale, in collaborazione con il RPD, compete il coordinamento in materia di privacy per il Consiglio regionale.

Tutti i Dirigenti, compreso il Segretario generale, il Vicesegretario generale (per strutture alle dirette dipendenze), il Capo di Gabinetto, **il Direttore responsabile dell'Agenzia Consiglio Notizie e il Portavoce**, assicurano il rispetto degli obblighi previsti dal GDPR e dalla normativa nazionale posta in capo al Titolare del Trattamento, per i trattamenti connessi all'espletamento delle funzioni di propria competenza individuate nell'ambito delle strutture cui sono preposti. In particolare essi sono tenuti a:

1. garantire il rispetto della normativa vigente e verificare la legittimità dei trattamenti di dati personali effettuati nella struttura di riferimento in modo che nessun trattamento di propria competenza sia svolto in violazione della normativa di riferimento (GDPR, Art. 6);
2. designare un proprio collaboratore in qualità di Referente privacy, dedicato anche a supportare il Dirigente stesso nelle attività di gestione degli adempimenti connessi alla protezione dei dati e a fungere da punto di contatto con il RPD e l'Ufficio privacy. La designazione è comunicata per conoscenza all'Ufficio competente in materia di organizzazione e personale, al RPD e all'Ufficio privacy;
3. è responsabile della predisposizione delle informative relative ai trattamenti di propria competenza con il supporto del RPD sulla base di modelli predisposti dall'Ufficio privacy;

4. collaborare con il RPD, fornendo le informazioni richieste anche al fine di agevolarne l'attività di controllo;
5. sovraintendere e vigilare sul rispetto delle norme in materia di privacy nell'ambito della propria struttura e impartire istruzioni dettagliate e precise per garantire che il trattamento dei dati personali di competenza sia eseguito in maniera corretta e conforme alle normative vigenti;
6. favorire quanto più largamente possibile la partecipazione ad eventi formativi in materia di protezione di dati personali da parte dei soggetti autorizzati;
7. collaborare, per quanto di competenza, con il Segretario generale e il RPD alla stesura delle linee guida per la progettazione di soluzioni di *privacy by design e privacy by default*, fornendo le informazioni richieste anche attraverso i propri Referenti privacy;
8. censire e aggiornare tempestivamente i trattamenti dati personali effettuati nell'ambito della struttura di competenza, dandone tempestiva comunicazione al RPD tramite l'Ufficio privacy, per l'aggiornamento del **Registro delle attività di trattamento**, (GDPR Art. 30) verificando in particolare:
    - la legittimità della base giuridica delle finalità;
    - l'opportuna applicazione delle misure di sicurezza adottate;
    - la corretta indicazione dei tempi di conservazione dei dati e l'eventuale necessità di chiederne la cancellazione;
    - la verifica del rispetto dei tempi di rimozione dei dati pubblicati su sito web;
9. effettuare ove necessario, la preventiva valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'articolo 35 del GDPR quando il trattamento dei dati personali può presentare un rischio elevato per i diritti e le libertà degli individui;
10. dopo aver effettuato la DPIA, trasmettere i risultati al RPD, affinché questi possa fornire il proprio parere, come previsto dall'articolo 39, paragrafo 1, lettera c) del GDPR. Il parere del RPD è un elemento importante per valutare se le misure adottate sono adeguate a proteggere i diritti degli interessati;
11. in limitate circostanze, il Delegato può decidere di limitare l'autorizzazione al trattamento a un numero ristretto di dipendenti, in base alle specificità del trattamento in questione. Questo può essere necessario, ad esempio, quando si tratta di dati particolari o quando l'accesso a sistemi informatici comporta la gestione di banche dati particolarmente delicate o riservate. In tali situazioni, è necessario redigere un atto autorizzativo specifico; questo atto autorizzativo deve essere documentato e conservato in modo da poter essere presentato in caso di controlli da parte delle autorità competenti.;
12. predisporre e fornire a terzi le informazioni relative al trattamento dei dati personali e garantire agli interessati i diritti riconosciuti dalla normativa, anche dando riscontro alle loro istanze, secondo quanto previsto dal GDPR;
13. segnalare al Segretario generale, al RPD e alle strutture competenti, i fatti o le situazioni anomale che possano aver comportato una violazione dei dati personali;
14. ciascun Dirigente sottoscrive gli accordi con i Contitolari e con i Responsabili del trattamento dei dati sulla base delle competenze del servizio di propria responsabilità.

Un ruolo specifico in materia di privacy è riconosciuto al Servizio Sistemi informativi e Affari Generali a cui compete:

1. Coordinare i rapporti con il Gestore di sistema informativo regionale e/o la società regionale *in house* di fornitura di servizi informatici e gli altri fornitori di prodotti e servizi ITC;
2. Adottare eventuali manuali tecnici per utilizzo in sicurezza delle risorse informatiche;
3. Designare i soggetti autorizzati al trattamento che svolgono, anche in via esclusiva, funzioni di Amministratori di sistema;
4. Effettuare periodicamente un monitoraggio dei soggetti autorizzati all'accesso alle banche dati informatiche, alle cartelle condivise e alle caselle di posta elettronica di gruppo, contenenti dati personali e, nel caso venga meno l'autorizzazione, avvisare il soggetto competente ad effettuare la disabilitazione.

4. AUTORIZZATI AL TRATTAMENTO

L'articolo 2 quaterdecies, comma 2, del Codice Privacy stabilisce che il Titolare del trattamento ha il compito di definire le modalità, attraverso le quali autorizzare le persone che operano sotto la propria autorità, ad effettuare il trattamento dei dati personali, in conformità con quanto previsto dall'articolo 4, paragrafo 1, numero 10 del GDPR.

L'Autorizzato è colui che, in qualità di persona fisica, esegue concretamente le operazioni di trattamento dei dati personali.

Tutto il personale assegnato al Consiglio regionale del Friuli Venezia Giulia, è autorizzato al trattamento dei dati personali di titolarità del Consiglio stesso limitatamente allo svolgimento dei propri compiti d'ufficio in base alle competenze proprie della struttura di appartenenza.

Questa autorizzazione è implicita nell'atto di assegnazione del dipendente alla specifica Struttura.

Il dipendente deve osservare scrupolosamente le Linee guida adottate e attenersi alle istruzioni impartire dal Delegato, affinché i trattamenti dei dati personali da lui eseguiti avvengano in maniera corretta e conforme alle normative vigenti; egli deve essere aggiornato sulle procedure relative alla protezione dei dati personali, nonché sulle eventuali modifiche normative che possano influire sui trattamenti autorizzati. In particolare negli articoli 29 e 32, paragrafo 4, del GDPR si sottolinea l'importanza che ogni persona che abbia accesso ai dati personali non li tratti senza essere stata adeguatamente istruita a tale scopo.

I dipendenti sono tenuti al segreto d'ufficio e vincolati alla riservatezza da specifiche disposizioni anche del Codice di comportamento dell'amministrazione regionale FVG.

In limitate circostanze, il dipendente può essere espressamente autorizzato dal Delegato a trattare degli specifici dati personali. Questo può essere necessario, ad esempio, quando si tratta di dati particolari o quando l'accesso a sistemi informatici comporta la gestione di banche dati particolarmente delicate o riservate. **In questi casi il dipendente viene incaricato per iscritto dal Delegato competente**, attraverso apposita lettera di autorizzazione in cui sono specificati i trattamenti consentiti e sono fornite idonee istruzioni relative alle operazioni da compiere e le regole comportamentali alle quali attenersi. Apposita comunicazione deve essere fatta anche ad eventuali tirocinanti qualora nello svolgimento dei loro compiti fossero incaricati di trattare dati personali di titolarità del Consiglio Regionale.

Il Dipendente, inoltre, nell'ambito dei trattamenti di propria competenza deve segnalare senza esitazione al Delegato i fatti o le situazioni anomale che possano aver comportato una violazione dei dati personali.

5. RESPONSABILI DEL TRATTAMENTO

Il ruolo del Responsabile del trattamento è chiaramente definito all'interno del GDPR (art. 4, par. 1, n. 8), è la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che tratta dati personali per conto del Titolare del trattamento.

Il rapporto tra il Titolare e il Responsabile del trattamento deve essere formalizzato attraverso un contratto o altro atto giuridico che vincoli il Responsabile al Titolare (GDPR art. 28, par. 3). Questo contratto deve essere stipulato in forma scritta e deve e stabilire gli obblighi specifici del responsabile, come l'adozione di misure tecniche e organizzative adeguate per garantire la sicurezza dei dati, l'assistenza al titolare nel rispetto degli obblighi normativi, e il trattamento dei dati solo secondo le istruzioni del titolare. Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate – in primis agli standard stabiliti dal Titolare - in modo tale che il trattamento soddisfi i requisiti previsti dal GDPR e garantisca la tutela dei diritti dell'interessato.

Inoltre, il Responsabile del trattamento può essere autorizzato a subappaltare alcune delle sue funzioni a sub-responsabili, ma solo con l'autorizzazione scritta del Titolare del trattamento. Questi sub-responsabili devono essere vincolati dagli stessi termini del contratto principale tra Titolare e Responsabile.

La Società Insiel S.p.A. è identificata come il Responsabile del trattamento dei dati personali di cui è titolare il Consiglio regionale FVG in base alle convenzioni Prot. GEN GEN 9483-A del 13 luglio 2018 e prot. GEN-GEN-6496-A di data 23 dicembre 2022, per i servizi relativi allo sviluppo e gestione del Sistema Informativo Integrato Regionale.

Ciò implica che Insiel S.p.A. tratta i dati personali secondo le istruzioni e sotto la supervisione del Titolare del trattamento ed è responsabile del rispetto delle norme del GDPR e della tutela dei diritti degli interessati.

6. REFERENTI PRIVACY

Ogni Dirigente designa un proprio collaboratore in qualità di Referente per la protezione dei dati personali, dedicato a supportare il Dirigente stesso nelle attività di gestione degli adempimenti connessi alla protezione dei dati e a fungere da punto di contatto con il RPD e l'Ufficio privacy. La designazione è comunicata per conoscenza all'Ufficio competente in materia di organizzazione e personale e al RPD.

I referenti lavorano in sinergia con il RPD e l'Ufficio privacy, per sviluppare e garantire l'adeguamento del sistema di trattamento dei dati personali del Consiglio regionale alla normativa vigente e in particolare a quanto disposto dal GDPR.

7. PERSONALE DEI GRUPPI CONSILIARI:

Il personale assegnato ai gruppi consiliari è autorizzato ai trattamenti di dati personali di cui è titolare il Consiglio regionale esclusivamente nello svolgimento delle attività istituzionali proprie dell'organo consiliare. Tali trattamenti devono avvenire nel rispetto delle disposizioni contenute nelle Linee Guida in materia di trattamento e sicurezza dei dati personali, emanate dall'amministrazione consiliare.

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: STEFANO PATRIARCA
*CODICE FISCALE: **********
DATA FIRMA: 17/05/2024 14:50:06

NOME: MAURO BORDIN
*CODICE FISCALE: **********
DATA FIRMA: 23/05/2024 13:10:33